

Volume 5:
Information Technology

TABLE OF CONTENTS

VOLUME 5: INFORMATION TECHNOLOGY

<i>a. Hardware and Software Platform</i>	<i>1</i>
<i>b. Operating System/Network Software</i>	<i>7</i>
<i>c. System Compatibility</i>	<i>18</i>
<i>d. Network Configuration and Architecture</i>	<i>22</i>
<i>e. Ability to Provide an Electronic Data Interface</i>	<i>31</i>
<i>f. System Downtime and Change Management Process</i>	<i>36</i>
<i>g. IT Personnel Training</i>	<i>40</i>
<i>h. System Data Archive and Retrieval</i>	<i>46</i>
<i>i. System Security and Audit Trail</i>	<i>49</i>
<i>j. Information Systems Data Mapping</i>	<i>53</i>
<i>k. Data Flows and System Edits</i>	<i>97</i>
<i>l. Testing Plan and Data Conversion</i>	<i>115</i>

a. Hardware and Software Platform

Our Information Services Department is integral to the overall vision of ValueOptions, and to that of the Maricopa County behavioral health system, by providing an exceptionally efficient, accurate, and secure means of communication and data management. We will describe in the paragraphs that follow, the ValueOptions hardware and software used through our diverse infrastructure and three main data centers located in Phoenix, Arizona, Reston, Virginia and Norfolk, Virginia.

The foundation of our information systems is a carefully constructed infrastructure with a state-of-the-art hardware platform that not only provides the capabilities to support the current behavioral health system but also handles the demands placed upon it as the behavioral health system continues to grow and change. In fact, our recently upgraded AS400 midrange server provides close to a 400% increase in production capabilities compared to our previous server. Applications on this system currently run at 35% of capacity and only 25% of the storage space is utilized, leaving ample room for growth.

This advanced hardware platform, along with innovative software developed by ValueOptions, allows us to provide more efficient ways of processing, storing and transferring information. For example, since ValueOptions was awarded the Maricopa County contract in 1999, claims processing turnover time has improved by 88% over the previous Regional Behavioral Health Authority (RBHA). Today we process approximately 65,000 claims a week, 250,000 claims a month, and 3.4 million claims a year—with a rate of 94% auto adjudication. In addition, 97% of all claims are being processed electronically. Because of the speed and accuracy of this system, providers receive encounter credit for their services or fee-for-service dollars faster. This process allows the providers more capital and balanced funding to maintain staff and to provide more services.

In addition to this powerful server, our platform also includes a high-speed Wide Area Network (WAN) that provides the structure for ValueOptions' newly developed electronic provider support network. This network, for the first time in Maricopa's history, links the majority of all large and several small providers to the RBHA's information systems, allowing these providers to log on to our system to get the information they need more conveniently and efficiently. (This network interconnectivity will be discussed in detail in section 5.d., which focuses on network configuration.)

Our platform includes an enterprise level telecommunications system that handles more than 550 incoming crisis line and customer service calls each day – the equivalent of 7,800 per week or 200,000 per year. This substantial telecommunications system has successfully handled a 6% increase in calls over the past year, and like the rest of our hardware platform, was purchased with a consideration for future growth. ValueOptions' continuous investment in advanced technologies ensures a scalable information systems platform to seamlessly provide services to our growing population.

Below, you will find details regarding ValueOptions' hardware and the platform on which it runs, as well as facility safeguards including environmental and physical security. We begin this section by providing information pertaining to the systems operated by the ValueOptions corporate offices in Virginia, followed by details about the Arizona Service Center and ValueOptions Direct Service Sites.

ValueOptions Corporate Systems – Reston, Virginia *(Primary Business Systems)*

Data Systems

ARTHUR: IBM AS400 840

Serves as the primary ABSolute and MHS Business Systems host.

Software:

Operating System: IBM OS400 V5R2.

Primary Applications: MHS and ABSolute. The application databases are DB2 Universal Databases.

Hardware and Fault Tolerance of the System:

Processing: 18-way IBM's iStar processors w/ Silicone On Insulator (SOI) chip technology.

RAM: 80GB

Storage: 3+ TeraBytes total disk space utilizing RAID5 disk protection.

Ethernet communication is supported by one 1Gbps NIC and three Fast Ethernet adapters (10/100 Mbps).

Hardware Warranty:

The hardware is protected with 24 hour per day, 7 day per week, and 365 day per year on-site support contract from IBM.

Backup Power:

This system is protected by an Uninterruptible Power Supply (UPS) in addition to a backup diesel generator responsible for providing power for the entire Data Center during an outage. Contracted vendors are in place to supply diesel fuel for extended power outages.

Corporate Data Warehouse: IBM RS/6000 7017-S80

Serves as primary ValueOptions Corporate data warehouse.

Software:

Operating System: IBM AIX 4.3.3.11.

Primary Application: Sybase.

Hardware and Fault Tolerance of the System:

Processing: 24-way 450 MHz processors

RAM: 12GB

Storage: 3 TeraBytes total disk space with NOS drives mirrored (RAID 1) and data drives configured as part of a fiber channel EMX 8430 Symmetrix SAN.

Ethernet communication is supported by two 1Gbps Ethernet Adapters.

Hardware Warranty:

The hardware is protected by means of 24 hour per day, 7 day per week, and 365 day per year on-site support contract from IBM.

Backup Power:

This system is protected by UPS standby power in addition to a backup diesel generator responsible for providing power for the entire Data Center during an outage. Contracted vendors are in place to supply diesel fuel for extended power outages.

Security Safeguards

The ValueOptions Data Center houses the above business-class servers in a secure Data Center. General building access is restricted to only ValueOptions employees and their escorted guests. All exterior doors require card reader access privileges. Cipher-lock doors secure the Data Center, as well as all IDF (Intermediate Distribution Facility) locations in this building. The data center has an additional layer of security in that access to this area of the building is further limited to only Computer Operations and Systems Administration support staff. The electronic key cards are individually assigned to ValueOptions' employees, and access is tracked.

All ValueOptions employees are required to wear a picture ID. A ValueOptions Information Services employee must escort all vendors and other visiting and/or non-ValueOptions Information Services employee into all secured areas. During non-business hours the main entrance into the ValueOptions suite is secured and also requires an electronic key card to gain entrance. The building is monitored 24 hours a day, 7 days a week by the Kastle Alarm System that will provide notification if an interior or exterior door is left open for more than 15 minutes. Additionally, building management provides an on-site security guard to patrol the public areas of the building and parking lot after-hours.

Environmental Safeguards

Fire suppression for the Data Center and the building in which the data warehouse resides is provided by a "pre-action" (dry-pipe) sprinkler-head system. The first floor Data Center is above grade and there are moisture detection sensors positioned throughout the Data Center flooring that alert operations staff to possible flood or moisture exposure. Two redundant 20-ton Liebert glycol high-capacity heating-ventilation air-conditioning (HVAC) units handle the Data Center temperature control. Humidity and temperature are constantly monitored, and threshold alarms are sent electronically to a computer operations employee, as well as to our third party security and environmental monitoring vendor. Power to the Data Warehouse Storage Area Network and application server is provided through fully redundant internal power supplies, with additional redundancy supplied by separate power feeds from two external Power Distribution Units. Both a UPS and a Caterpillar 425KW diesel generator with over 72 hours of fuel supply support the Data Center.

ValueOptions Corporate Systems – Norfolk, Virginia
(Backup Business Systems)

Data System

Backup IBM AS400 740

Serves as a redundant host for the MHS business system.

Software:

Operating System: IBM OS400 V5R2.

Primary Application: MHS as a redundant system. The MHS application database is DB2 Universal Database.

Hardware and Fault Tolerance of the System:

Processing: 12-way Pulsar technology processors

RAM: 40GB

Storage: 3+ TeraBytes of disk space utilizing RAID5 disk protection.

Ethernet communication is supported by two Fast Ethernet Adapters (10/100 Mbps).

Hardware Warranty:

The hardware is protected with 24 hour per day, 7day per week, and 365 day per year on-site support contract from IBM.

Backup Power:

This system is protected by an Uninterruptible Power Supply (UPS) in addition to a backup diesel generator responsible for providing power for the entire Data Center during an outage. Contracted vendors are in place to supply diesel fuel for extended power outages.

Security Safeguards for Backup Systems

During normal business hours, the Data Center is located behind two sets of cipher-lock security doors. After business hours, there are additional layers of security consisting of swipe badges for building access plus touch panel codes for the elevators. There is also an on-site security guard provided by building management. All door and elevator codes are changed periodically.

Environmental Safeguards for Backup Systems

Everything in the Norfolk Data Center is attached through a three panel Power Distribution Unit to a 100KVA UPS running at less than 50% capacity. All data center circuits are dedicated. The entire Norfolk office building housing the data center is on a diesel-powered generator that can operate for approximately 48 hours without refueling.

Both the buildings' HVAC, as well as four independent HVAC units, supply the data center with 16 tons of cooling for temperature control. Each unit has alarms for high temperature, high head pressure and water leakage. Since the units are independent, cooling continues even if one or more units are down.

Data center fire suppression is provided by an FM200 (Hepta Flora Propane) system complete with ceiling and under-floor detectors and dischargers.

ValueOptions Arizona Service Center (Maricopa County RBHA)

Data Systems

(See figure 5a-1 for a visual illustration of ValueOptions' business systems platform)

VO-PHX-DWH1: HP NetServer/H6000

Serves as a data repository for the Arizona Service Center.

Software:

Operating System Platform: NT 4.00 SP 6.0a

Primary Application: Sybase Server 11.5

Hardware:

Processing: 4-way Xeon 550MHz processors

RAM: 2.048GB

Storage: 300GB total disk space comprised of four 9.0GB and fifteen 17.0GB hard drives.

Ethernet communication is supported by two Fast Ethernet adapters (10/100 Mbps).

System Fault Tolerance:

Two of the 9.0GB drives are mirrored (RAID 1). They house the boot partition (500MB) and the NOS partition (8.5GB). Three 17.0GB drives are combined into a volume set (RAID 0) and the remaining hard drives are each configured as independent volumes.

Backup Power:

1-hour UPS standby power.

VO-PHX-SQL01: Dell Power Edge 8450

Serves as the local data warehouse.

Software:

Operating System: Windows 2000 Advanced Server Service Pack 4.0.

Primary Application: SQL Server 2000 Service Pack 3a.

Hardware:

Processing: 8-way Xeon 700 MHz processors

RAM: 8.192GB

Storage: 980GB total disk space comprised of two 18GB and thirteen 72GB hard drives.

Ethernet communication is supported by four Fast Ethernet adapters (10/100 Mbps).

System Fault Tolerance:

The two 18.0GB drives are mirrored (RAID 1) housing the boot partition (4.0GB) and NOS (13.0GB). Nine 72GB drives comprise the first of two database work spaces (RAID 5) with three additional 72GB drives comprising the second (RAID 5). One 72GB drive is partitioned as an independent volume with one additional 72GB drive in standby as a "Hot" spare.

Hardware Warranty:

The hardware is protected with 24 hour per day, 7day per week, and 365 day per year on-site support contract from Dell. Contract provides for a 4-hour response time.

Backup Power:

1-hour UPS standby power

Telephone Systems**Meridian 1 - Option 61C**

A Meridian 1 is a circuit-switched digital telephone system that provides voice and data transmission, capable of supplying service to 1,000 agents.

Software:

Operating System: Release 23

Additional Software Features: Primary Rate Interface (PRI) provides Caller ID, Automatic Call Distribution (ACD) allows multiple agents to accept a large number of calls from a single in-bound number.

System Fault Tolerance

The two Core/Network Modules are fully redundant, mirroring to each other.

Meridian 1 Sub-Systems

Meridian Mail

A digital voice mail system that provides menu driven directions and routing to help the incoming caller connect to the desired department.

Software: Version 12

Meridian MAX

Meridian MAX provides both real-time statistics, displays historical reporting on the call center operation and Automatic Call Distribution (ACD) configuration management.

Software: Version 8

Comverse Ultra Voice Recorder

Provides 24 hours a day, 7 days a week voice recording to 79 phones located in the Crisis, Customer Service, and Access departments to monitor for proper customer service and for legal documentation.

Software: Version 6.6

Security Safeguards

Primary Data Center

The Maricopa County RBHA houses the main business system servers and telecommunication systems in a secured Data Center located in the Phoenix Administrative Offices. Cipher-lock doors secure the Data Center, as well as all IDF (Intermediate Distribution Facility) locations in this building. Only selected Information Services employees have access into the Data Center. An electronic key card door, providing another layer of separation from the general public, also secures the outer area surrounding the Data Center. The electronic key cards are individually assigned to ValueOptions' employees, and access is tracked internally. In addition, all ValueOptions employees are required to wear picture identification. A ValueOptions Information Services employee must escort all vendors and other visiting and/or non-ValueOptions Information Services employees into all secure areas. During non-business hours the main entrance into the ValueOptions suite is secured, and an electronic key card is required to gain entrance. Additionally, building management provides an on-site security guard to patrol public areas of the building and parking lot after-hours.

ValueOptions Direct Service Sites

In addition to the systems housed in the Phoenix Administrative offices, each Direct Care Site has a secure MDF (Main Distribution Facility) where each site's telecommunications switch, data switch and routing equipment are located. These facilities are located in access-controlled areas of the Direct Care site behind cipher-lock doors. Each site has a security guard on duty during business hours. To gain access to controlled areas, employees must have a picture ID badge, and all non-employees must be escorted at all times. Sites have "panic buttons" in each of the doctor, nurse, and reception offices, and also have monitored alarm systems after-hours.

Environmental Safeguards

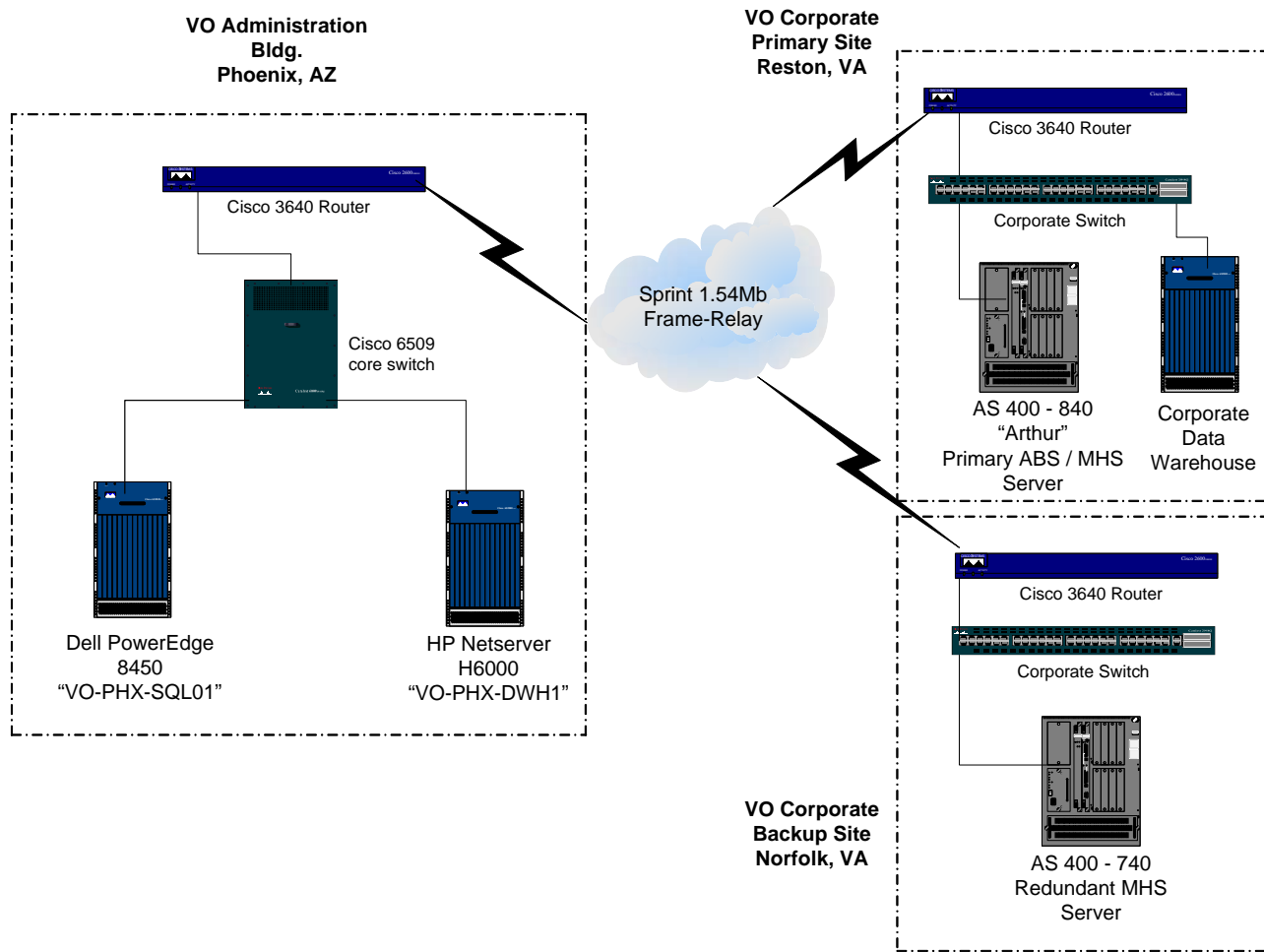
Primary Data Center

Temperature control to the Data Center is provided by two independent HVAC systems with thermal sensors tied to the building alarm system to safeguard against overheating. The HVAC systems also have a drip detection and alarm system to detect water leaks. Power is provided to the data warehouses via two independent dedicated power circuits. Additionally, they each have a UPS with up to one hour of battery backup. Fire suppression is currently provided by a water-based suppression system that uses proximity sprinkler heads, so that only sprinkler heads in the immediate area of a fire will activate and not the entire system. A non-water based replacement system is currently planned for early 2004.

ValueOptions Direct Service Sites

The Direct Service Sites do not contain equipment that is as sensitive to temperature and environmental factors. The sensitive equipment is located in the Primary Data Center. Therefore the ValueOptions Direct Service Sites do not require the same level of protection. Building HVAC, with extra venting provided to the more enclosed areas, provides temperature control in these locations. Existing water-based suppression systems in each building provides fire suppression. Power is provided through dedicated circuits located in each MDF. Equipment is also connected to a UPS, providing temporary backup power and surge protection.

Figure 5a.1 Connectivity between Arizona Administrative Offices and Corporate Office



b. Operating System/Network Software

The ValueOptions Information Services Team has developed a wide array of innovative, fully integrated technologies designed to support the delivery and management of behavioral healthcare to all populations served by the Maricopa Regional Behavioral Health Authority (RBHA).

All software modules described in this section have been designed and continue to be enhanced to support clinical best practices, continuity of care, planning and development, service integration, and improved data transfer and processing. This is achieved by using software with maximum flexibility, allowing us to customize applications to meet our client's exact needs in a timely and efficient manner. This software, combined with our advanced database design, ensures a highly reliable, efficient data management system.

The Information Services teams' goal is to use technology to create a more efficient, more effective system overall by automating processes to save time and resources and by providing clear, well-organized data reports to assist management staff in evaluating and improving our administrative and clinical care systems.

The following section provides details about ValueOptions' operating system, database management system, programming language, and customized software applications.

Database Platform and Operating System

Our database design provides a solid, reliable foundation that is capable of handling the complex data management needs of over a thousand end-users, including providers, clinical staff, and administrative staff in all ValueOptions' departments.

This database operates within the IBM OS/400 operating system version 5.2, and has been built to take full advantage of our DB/400, a DB2 compliant database. IBM's DB2 is one of the most powerful and stable database engines in the world today. In conjunction with our comprehensive database design, this operating system enables us to provide an extremely rapid and user-friendly way to manage and process data.

In addition, our database is approaching a fully relational, fully normalized product—meaning that data that is entered is accessible automatically throughout the system and across all applications on the database, without duplication of data. This approach ensures the consistency of data, reduces data entry, and minimizes opportunity for error.

Finally, we take full advantage of our system's power and flexibility through the use of multi-level relational editing; a process of data verification that ensures that data entered into each field is consistent with other information that has been entered. This feature provides feedback to the end-user so that corrections can be made prior to submission of the data.

Software Development Tools: Programming Languages for Customized Solutions

ValueOptions owns the source code and has the expertise and resources to maintain and enhance all software used for core business systems. This allows us to offer software solutions customized to the needs of Maricopa County. The majority of these programming and development resources are located in our Arizona Service Center.

We utilize a variety of programming and development tools to create an efficient and technically advanced software development system. These tools have been carefully chosen to match the level of complexity and flexibility needed by all those who depend on it. Below is a list of the tools we have incorporated into our system:

<u>Development Tool</u>	<u>Vendor</u>	<u>Application Area</u>
COBOL	IBM	Managed Healthcare System-core administrative system
Advantage 2E	Computer Associates	ABSolute-core direct service module
J Walk	Seagull	ABSolute
Transact SQL	Microsoft	Data Warehouse
Crystal Reports	Seagate	Reporting
.NET	Microsoft	Reporting
COGNOS	COGNOS	Reporting

These applications provide flexible and easily customizable ways to manage, develop, and constantly improve our information system services. Tools like .NET help us to develop applications and make system changes quickly and easily. COGNOS

allows ValueOptions employees the ability to query, analyze, and report data relevant to their functions. Together these tools ensure a faster, more efficient service for the Maricopa County behavioral health system.

ValueOptions Information Systems Software Application Modules

Enrollment, Assessment, and Disenrollment Module

The Enrollment, Assessment, and Disenrollment (EAD) module ensures the accuracy of eligibility data for consumers entering treatment. Like all our modules, our EAD module is integrated with all other ValueOptions applications, not only allowing end-users to access information on consumer eligibility data, but also connecting them with other data sources such as references, benefits, contracts, claims, providers and authorizations. Access Line, Customer Service, and Contracts employees can all access consumer enrollment and eligibility data in order to research and resolve problems, and to rapidly procure needed services for which consumers are eligible.

Some of the basic features of this module include:

- on-line and batch consumership entry processing,
- on-line changes with history archival,
- automatic retroactive capitation/billing based on consumership changes,
- multiple provider selection per consumer,
- multiple option/benefit packaging per employer group with network,
- integrated general ledger by company/group/benefit parameters,
- integrated correspondence generation capabilities,
- user defined consumership edits and reporting,
- free form message tracking for inquiry and reporting, and
- user defined service edits by consumer/group to control adjudication.

The EAD module currently complies with all requirements of the Arizona Department of Health Services/Division of Behavioral Health Services (ADHS/DBHS) Request for Proposals, the CIS Manual, and HIPAA regulations.

Provider Network Credentialing and Contract Management Module

The Provider Network and Contract Management module supports processes involving provider entry, fee arrangements, service pricing and controls, reports, inquiry, and other functions that support the requirements of a managed healthcare organization. The system provides parameters for issues such as payment or service type and limitations, which can be used to control processing requirements. Some basic features found in the provider subsystem include:

- integrated multi-tiered provider credentialing management,
- multiple vendors per provider for payment processing,
- flexible provider numbering – up to 15 characters,
- multiple company processing capabilities,
- multiple provider reimbursement capabilities,
- integrated correspondence processing,
- flexible capitation payment processing,
- year end 1099 processing for all providers, and
- user-generated follow-up processing.

Providers are added to the system with associated accounts payable vendor information, fee schedules, discounts, and service restrictions. Provider data is also utilized in the claims adjudication process.

Authorization Management Module

The Authorization Management Module provides the ability to create, locate, and manage service authorizations for individual consumers. Authorizations are required for higher levels of care, such as inpatient, based on established clinical care criteria. Without an authorization, provider claims for these levels of care are denied. Denials are associated with a denial code that identifies the reason for the denial. A consumer's complete authorization history is maintained, and Care Managers have access to authorizations from both the Claims Subsystem and the Care Management modules.

Claims Processing Module

The Claims Processing Module supports the related processes of claims entry, adjudication, payment and reporting. Utilization Review (UR) capabilities are also included in the Claims Processing Module to support the basic needs related to productivity, analysis, and management, while the more detailed UR component is a separate system unto itself. Some of the features found in the claims processing subsystem include:

- on-line authorization/adjudication capabilities,
- efficient HCFA-1500 and UB82/92 screen entry formats for high volume processing,
- unlimited claim lines per claim,
- specific/generic service authorization capabilities,
- automatic matching of claim activity to outstanding authorizations,
- user and contract defined processing edits,
- automatic correspondence generation,
- on-line/batch claims adjudication capabilities,
- claim status history throughout the claim lifecycle,
- follow-up capabilities for claims and authorizations, and
- split payment and consumer reimbursement capability.

ValueOptions' information systems have been modified to support and comply with all HIPAA and State of Arizona regulations. Additionally, in an effort to support the seamless transition to the new HIPAA standards, ValueOptions will continue to support the National Standard Format (NSF), in addition to the new HIPAA transaction sets, for all providers who demonstrate a good faith effort to comply with the HIPAA mandated transaction sets.

Utilization Review Module

Our Utilization Review Module provides for the extraction and examination of claims, consumership, and provider activity over a specified period of time. This is accomplished through a series of management reports that describe the utilization of services by consumer groups and individual consumers. Our flexible format allows us to identify and track both the utilization of services by consumers and the patterns of service delivery of providers.

We also utilize a sophisticated system of reporting components using COGNOS, Crystal Reporting, and .Net. These solutions assist management in improving corporate and provider performance by informing everyone involved of the key steps in the management cycle including planning and budgeting, contracting, measuring and monitoring performance, managing service utilization, and evaluating outcomes. Our reporting component supports key management activities with a complete solution that spans all of the essential components of performance enterprise planning, score carding, and business intelligence. Currently we have over 400 management and key business indicator reports available to staff, providers, and other stakeholders.

Correspondence

The Correspondence Module is integrated with the Consumer Module to provide easy, automatic and manual generation of required correspondence. Each entry can have assigned effective and expiration dates to control subsequent adjudication.

Financial Modules

The Financial System interacts with the processing of the Accounts Payable, Accounts Receivable, and General Ledger activities. The system is designed to provide stand-alone financial transaction processing, or to serve as an integral part of the ValueOptions Information System.

The Accounts Receivable module supports processes related to invoicing, adjustments, and payments for supplied services and/or products. The basic components of the accounts receivable system are the entry, inquiry, and reporting aspects typically found in an accounts receivable system, along with the ability to receive generated invoices from other system components (e.g., Order Entry, Premium Billing). Company selected parameters control the requirements for processing (e.g., history retention, period processing, etc.) based on criteria that reflect the needs of the organization.

Accounts Payable supports processes related to invoices, adjustments, and payments for supplied services and products. The basic components of the accounts payable system are the entry, inquiry, and reporting aspects typically found in an accounts payable system, along with the ability to receive the generated invoices from other system components. Basic features include:

- vendor number and name search available during invoice processing,
- flexible vendor number assignment with up to 15 characters,
- vendor payment terms automatically calculating discounts and due dates,
- consolidation vendor capabilities for payment processing,
- on-line check reconciliation for both system and manually generated checks,
- multiple company processing capabilities,
- multiple General Ledger (G/L) Cash and Accounts Payable accounts,
- unlimited voucher distribution, and
- recurring voucher capabilities.

The General Ledger Module provides for the accumulation and reporting of journal entries in up to 12 separate accounting periods. The basic database consists of the general ledger master containing all general ledger account numbers, as well as periodic balances and balance forward amounts. The transaction file contains all detail journal entries for the user specified retention period. The system is designed to stand-alone or to interface with other subsystems. Data may be reported separately or in consolidated form for up to 99 companies. Account number format is user defined and is independent of reporting capabilities.

Security System

The Security System allows the maintenance of the application and user system security. The basic database consists of the Security Master containing all users, along with an Application Master containing all available systems and applications. Security is based on layers to prohibit personnel from unauthorized altering, destroying or disclosing of sensitive data. Access to applications and data is controlled by permissions setup in the systems Access Control Lists (ACL). System access is controlled through permissions defined in a user account. Access to the user account is controlled through the use of identification and authentication techniques. This security system fully supports role-based access, ensuring compliance with HIPAA requirements for minimum necessary access to information. This module also performs tracking and logging for auditing purposes.

The core of the system is in the definition of the users and applications in which access and processing is controlled. The system administrator has responsibility for establishing the departments, users, and for cross-referencing these to the applications for processing.

Interactive Voice Response System

The Interactive Voice Response (IVR) System offers eligibility verification on enrolled consumers for providers on a real-time basis, allowing them to access this data 24 hours a day, 7 days a week through a separate toll-free number. ValueOptions has received the Sixth Annual Excellence in Healthcare Risk Management Award from Modern Healthcare magazine for our IVR clinical application. This award recognized ValueOptions for innovation in providing ease of access to services for consumers and autonomy for network providers, resulting in overall improved coordination of services.

IVR is an automated voice information inquiry system through which providers can access selected information via telephone. All consumer information, including eligibility information, is initially loaded into our ValueOptions Management Information System (VMIS) and is integrated with both the Claims and Inquiry Tracking modules. Once eligibility information is entered into VMIS, eligibility information is available to the IVR. As it is currently implemented, the service also allows in-network providers to register outpatient care.

The following list details the information a provider can access through the IVR:

- consumer's benefit information,
- consumer's eligibility status,
- claims status,
- automated faxed copy of consumer's eligibility status,
- automated faxed copy of claims status, and
- automated faxed copy of consumer's benefit information.

The IVR system and our web enabled e-Provider Partner permits provider access to:

- check claims payment status,
- verify eligibility,
- check benefits,
- register care (if included in the delivery model), and
- request Authorizations (e-Provider only, currently under development).

Inquiry Tracking

The Inquiry Tracking module provides the capability for on-line referral tracking. The referral-tracking feature in VMIS allows users to access a provider search engine to identify providers by location, discipline, and clinical area of expertise. The system also tracks the caller's provider preferences and documents whether these were met. This module was designed to offer the care manager efficient data collection and tracking capabilities. On-line entry of clinical data, with maintenance of clinical case history, allows the care manager to easily enter and access all clinical information, including:

- referral priority (urgent, priority or routine),
- reason for call (access to services, claims, or benefits),
- complaint calls (service, plan, or provider related),
- disposition of call (complete or follow up),
- nature of call (information, status, or complaint),
- identification and type of caller (consumer, provider, provider staff, or family consumer),
- inquiry type,
- response requirements (urgent – one business day, checks for week ends and holidays),
- enrollment/eligibility or stakeholder record (calls are attached to the caller and all calls can be reviewed),
- work flow management (uses work queues to manage responses, e.g., a claims adjustment), and
- the customer service representative documents request and the inquiry is sent to the claims queue.

When tracking written correspondence such as complaints and grievances, the system also enables tracking of the date the response letter is mailed to the consumer. Clinical appeals data include clinical notes as part of the tracking information gathered during the appeals process. The clinical case is separate from the inquiry record to ensure patient confidentiality.

The Inquiry Tracking Module (ITM) supports workflow management between departments. This module supports the capture of inquiry data and distributes it to the responsible individual or department for resolution. It maintains the inquiry details throughout resolution and keeps historical maintenance of all inquiries for all participants. As a Care Manager friendly management system, ITM prioritizes the Care Managers' daily workload in-box and serves as an electronic tickler system to remind ValueOptions personnel when a promised response is due.

Electronic Data Interface (EDI)

The Electronic Data Interchange (EDI) module handles all electronic claims as well as encounter and eligibility data exchange. ValueOptions has created a centralized program, PRIDUS, which allows providers to send and receive the following information in an electronic format:

- 837 Professional and Institutional file submission errors,
- 835 Explanation of Benefits,
- 834 Enrollment and Demographics,
- 834 Enrollment and Demographics file submission errors,
- 834 Enrollment and Demographics accepted records, and
- 834 Enrollment and Demographics rejected records.

Consumer Care Management Data-ABSolute Module

By compiling data about consumers, we are able to measure not only the consumer's progress and outcomes, but our own organizational processes and outcomes as well. Through our extensive database, we are able to track information that is then used to develop better ways to serve consumers. The following sections show the information we capture to ensure that we are giving the best possible care to consumers and the best management tools to our staff.

Application Tracking System

The Application Tracking System (ATS) supports the timely staffing of open case management positions to insure that appropriate consumer-to-case-manager staffing ratios are maintained. This module includes the following features:

- case ratio/need-based staffing analysis,
- job description maintenance,
- position requisition,
- position posting,
- internal and external applicant tracking, and
- multilevel electronic approval tracking.

Case Management Desktop

The Case Management Desktop module supports all facets of clinical case management, including:

- caseload management,
- critical timeframes on the completion of all assessments, treatment plans, progress documentation, and ADHS-mandated data sets for enrollment, disenrollment and assessment,
- alerts created by the crisis and jail diversion modules,
- online audit summary of overall caseload performance, and
- transition ticklers.

The Case Management Desktop module supports drill-down access to all aspects of a consumer's clinical record related to performing the function of case management.

Progress Notes

The Progress Note module supports the full documentation of all aspects of consumer care and includes the following features:

- multiple formats (RAPP and PIPP),
- custom defined formats,
- secured psychiatric notes,
- billable notes, and
- spell check.

Status Log

The Status Log module tracks all consumer related events based on date, time, event type, and related agency. Events can be entered manually or can be auto-populated from other modules. The Status Log supports a series of access to care timeframe reports.

Treatment Planning

This module helps define and measure consumers' individual/customized treatment plan by helping clinicians document individualized goals and objectives.

- problems, goals, objectives, methods, and services hierarchies,
- target dates,
- progress measures,
- collaboration note pad,
- multiple approval levels, and
- tracking of unmet needs.

The next release of the Treatment Planning tool in Arizona, which is currently being used in other ValueOptions service centers, includes the following:

- custom formatting and plan levels,
- multiple treatment plan formats,
- support for clinical pathways,
- linking of progress note to treatment plan,
- pdf printing, and
- cross association across treatment plan levels (i.e. methods to multiple objectives).

Face Sheet

The Face Sheet module supports the presentation of consumer clinic record information, which includes:

- demographics,
- alias names (akas),
- related people,
- provider relationships,
- family relationships,
- eligibility,
- insurances,
- legal/court orders,
- tracking elements, and
- custom fields.

Jail Diversion

The Jail Diversion module supports the identification of incarcerated consumers and notification of their incarceration to the Jail Diversion team and associated Case Managers. This module is supported by an electronic exchange of information between the VMIS and the Maricopa County Jail Booking System. At defined intervals, the Jail Diversion module queries the Jail Booking system for enrolled incarcerated consumers. It implements a multiple tier identification algorithm that identifies absolute matches and partial matches. Partial matches are presented to the Jail Diversion team for resolution. When a match is found, the Jail Diversion module transfers information that identifies the court, hearing date, and up to three charges to the VMIS and notifies the associated Case Manager.

Crisis Triage

The Crisis Triage module supports the Maricopa countywide behavioral health crisis response system. This module is utilized by not only the ValueOptions Crisis Team, but also by contracted crisis providers through a secure web interface, to support the coordination of care. This module features the following functions:

- multiple search for consumer, which includes a soundex (sounds-like) search criteria,
- access to full episode history,
- access to the at risk crisis plan,
- lethality scales,
- mobile team dispatch,
- response timeframe tracking,
- wellness checks,
- crisis notes, and
- case manager notification of the crisis episode.

Practice Management

The Practice Management Module supports all provider support functions, which include:

- staff and resource scheduling,
- system-wide centralized scheduling,
- authorization tracking against scheduled and encountered services,
- service ticketing,
- billable progress notes,
- charge entry,
- professional services billing (paper or electronic NSF or HIPAA 837P),
- secondary billing,
- reconciliation of payments and adjustments,
- electronic reconciliation (HIPAA 835),
- extensive productivity, billing, and reconciliation reporting, and
- browser based/web enabled (128 ssl encrypted).

Housing and Residential

The Housing and Residential module supports the tracking and administration of housing and residential opportunities for consumers. The module functionality includes:

- living situation tracking,
- housing application entry,
- placement tracking,
- grant tracking,
- residential application entry,
- wait list management, and
- reporting which includes the HUD APR.

We currently provide collaborative access to this module to ValueOptions' major housing provider agency.

Site Management

The Site Management module includes the following features:

- caseload Staffing Analysis to support appropriate case staffing levels based on target staffing ratios,
- online Audit Summary of Site and Team performance on key timeframes,
- staff Assignment/Staffing Changes, and
- reporting.

Custom Forms

The Custom Forms module supports the development of forms and clinical workflows. This module also supports the following features:

- security,
- approval hierarchies,
- conditional branched questions,
- embedding of other application modules, including substance tracking, diagnosis, and medications,
- data validation,
- review intervals and ticklers,
- electronic signatures,
- limited values,
- multi-selection values, and
- form status tracking.

Health Information Access and Accounting

The Health Information Access and Accounting module supports the tracking and management of Protected Health Information (PHI) based on the processes and timeframes prescribed by HIPAA. This module supports the following functions:

- disclosure tracking,
- privacy practices,
- PHI amendments,
- PHI disclosure accounting,
- privacy protection,
- consent for release of information, and
- disclosure accounting statements.

Electronic Clinical Record

A number of technologies have been integrated to support a system-wide total electronic clinical record. Additionally, the VMIS will continue to be enhanced to support real-time, two-way sharing of clinical record information with treating providers. An example of this is our recent implementation of a link to META's Metbase system to share Crisis Psychiatric Assessments and Notes. The second phase of this project will include expanding our ability to share medication information.

Policies and Procedures on Software Upgrades: ValueOptions Information Systems Change Management Process

ValueOptions defines our software upgrade policies and procedures through a Change Management Process (CMP). This process governs changes related to the development of new systems, enhancements made to existing systems, and technical support. ValueOptions CMP objective is to ensure that a standardized, effective and efficient process is in place for the intake, approval, prioritization and fulfillment of requests for service received by the Corporate Information Services Department. The CMP controls, prioritizes, and streamlines the delivery of changes to our Information Systems products and services. Our formal CMP has been in place for several years and includes a published CMP manual, and the associated policies and procedures, to govern and guide participants through the process. Policies and procedures and associated forms and documents are published on our company web site that is available to all ValueOptions employees.

The Corporate Information Services and Business Support Department functions as the Change Manager. The CMP consists of ten main phases/components starting with the request initiation and ending with post go-live procedures. Metrics such as man-hour expenditures are captured in our CMP Tracking System in order to measure the effectiveness of the process.

Phase 1 – Request Initiation

All user requests for Information Services development and changes are directed to the Technology Call Center (TCC) or “Help Desk”. Requests may be submitted via paper form, phone call, or via email. Any Information Services Managers identifying internal requests may initiate the CMP without contacting the TCC. All requests are entered into our Service Tracking System, known as HEAT, either by the receiving TCC Technician or by the initiating Technical Manager. The TCC Technician uses standard protocols to identify the request as either a problem report or a request for new development or enhancements to our systems. Any request identified as a problem is managed according to our Problem Escalation protocols and is handled appropriately based on the severity of the problem. “Non-problem” or “non-Help Desk” requests are sent the appropriate technology owner, typically a Business Analyst, for further evaluation.

Phase 2 – Business Support Analysis

When the Technology Owner or Business Analyst receives the request, a determination is made regarding the request: Should the request be considered? Should the requested project be categorized as a capital project? Are there any similar or related existing requests in the queue? Does the request require a return-on-investment (ROI) analysis and submission to the Information Services Governance Board for review and approval?

Based on this analysis, the Business Analyst may terminate the request, initiate action to implement the request, or escalate the request to the Information Services Governance Board for review and approval. Any request that requires the commitment of funds in excess of a specified dollar threshold, that has a duration of greater than a specified time period, that affects the entire system, or that affects multiple service centers, must be submitted to the Information Services Governance Board for review (See Phase III below). Projects that do not require Information Services Governance Board approval advance to Phase IV.

Phase 3 – Project Approval and Design when Information Services Governance Committee Approval is Required

Once the Business Analyst determines that Information Services Governance approval is required, the Business Analyst assists the original requestor to compile a written scope and justification for the project. Once the scope and justification documentation is completed, the Business Analyst reviews the documents and may suggest changes to the requestor. When the review and modifications are completed, the requestor and Business Analyst present the request to the Information Services Governance Board. If the request is denied, the request is terminated. The requestor has the option to “rework” the request and start the process again.

If the Information Services Governance Board approves the request, it is prioritized and becomes an approved project. A Project Manager is assigned and a high-level work plan with timelines, milestones and resources is developed. A Functional Specification Document is prepared, reviewed and approved. Next, the Application Owner and System Analyst prepare a Technical Design Specification for review. Once finalized the original requestor and Business Owner sign off on the technical specifications and the project is placed under configuration management.

Phase 4 – Project Approval and Design when Information Services Governance Board Approval is NOT Required

For requests that do not require Information Services Governance approval, the Business Analysts determines whether the request is for application development or is an Operations request. Operations requests typically do not involve an application or hardware upgrade. For projects that are application requests, the Business Analysts coordinates the development of a functional specifications document with the Business Owner, Application Owner, Technical Contact and Systems Analysts.

Once completed the requestor must approve the document. Next, the Information Services development team is notified of the request and the task is prioritized, scheduled and resourced, and a Technical Design Specification is developed and approved.

Phase 5 – Operations Request

An operations request typically involves efforts required to implement non-applications and hardware-type changes. The request is forwarded to the proper Operations Owner for review and is either approved or denied. If approved, the Operation Owner prioritizes and schedules the project based on the requirements. The Chief Administrative Officer must approve and sign off on the request. Once Vice President approval is received, a Project Manager is assigned and the task is initiated and project managed through completion.

Phase 6 – Development Change/Control

Once a project is approved, the Development/Change Control Process is initiated. The assigned technician submits a Production Change Form to the Change Control Manager to secure the modules, libraries, workspace, and development environment needed to fulfill the request. The Change Control Manager fulfills the requested items specified in the Production Change Form and notifies the Technician that the requested resources are ready. The coding process begins to fulfill the project request as outlined in the Technical/Design Specification.

Phase 7 – Testing and Acceptance

A Test Plan is created that identifies all phases of the required testing process (Levels 1, 2 & 3), the participants involved, the system modules/screens, test scenarios, data used in the tests, and the expected results. All involved parties review, modify and approve the Test Plan. In Level 1, the Technician completes unit testing and checks for reasonable results. The modified modules are moved to locations that permit integrated testing. In Level 2 testing, an integrated test is performed to check that the modifications are compatible with other components of the application or with external system interfaces. Level 3 involves User Acceptance testing. The users test the modifications using applicable business processes. This level of testing ensures that the modifications do not detract from system functionality and that the application will perform successfully under realistic business environments.

The results of each test are documented and compared to expected results as noted in the test plan. Issues are logged and categorized on a Test Phase Issue List, and are then reviewed by the project team member. Decisions are made regarding the test outcomes and whether or not changes are needed in the design and modifications. Finally, the Business Analyst Business Owner, Application Owner, Operations Manager, Developer, Requestor and other project team members determine whether to accept the modified product. After acceptance testing and approval, the Executive Sponsor reviews and approves the project.

Phase 8 – Training and Documentation

During the development process a comprehensive training plan is developed that includes the training curriculum, materials, session content, exercises, competency testing, trainer designations, facilities and schedules. Release Notes are developed to announce the new system features, functionality and patches, and then training is conducted according to the plan. Competency testing ensures that the training plan is effective and that the participants acquired the knowledge and skills included in the course content. If training is determined to not be effective, the application cannot “Go Live” until trainees demonstrate the necessary competence.

Phase 9 - Release

A plan is developed, which details all the necessary steps to move the change into production. Included in the plan are code copies, backup procedures, communications plan, contingency plan, operations notifications, finalization of project documentation, final hardware/software checklists, support team call list, and “Go Live” checklist and event schedule. The Production Change Control Process is then initiated. The Technician and Developer submit the code to be moved into production by the Change Control Manager. The Technology Call Center protocols are implemented to assist the TCC Technicians in supporting the newly implemented change. The Change Control Manager moves the new code into the production system and the change is now executed.

Phase 10 – Post Go-Live

Technical employees assess the success or failure of the move to production by evaluating initial system performance. The technical staff, users, and management evaluate the project outcome to determine whether the outcome is consistent with the initial goals and objectives. Final signoff of the Initiative Cover Sheet indicates the requestor’s acceptance of the project’s outcome and fulfillment of the request. In the event of a future failure, the problem escalation process is followed. The new implementation is now considered part of the base line product and is classified as being in support and maintenance mode.

c. System Compatibility

Maintaining compatibility between ValueOptions' Information Systems and provider systems is vital to making electronic data transfer and processing possible. However, the Information Services Team strives to take compatibility to the next level—not only making it possible for us to electronically communicate with our providers, but continually making this process easier and more efficient.

The basis of this advanced compatibility is a well-designed network architecture combined with innovative applications that the Information Services team has developed to better serve Maricopa County. These applications include the Provider Reporting Information Download and Upload System (PRIDUS) and HIPAA compliant Electronic Data Interface (EDI) software. In addition, we help make provider Information Systems more compatible by working directly with provider staff at their locations, enlisting our staff and technical services to help reconfigure their systems to work more efficiently with ours.

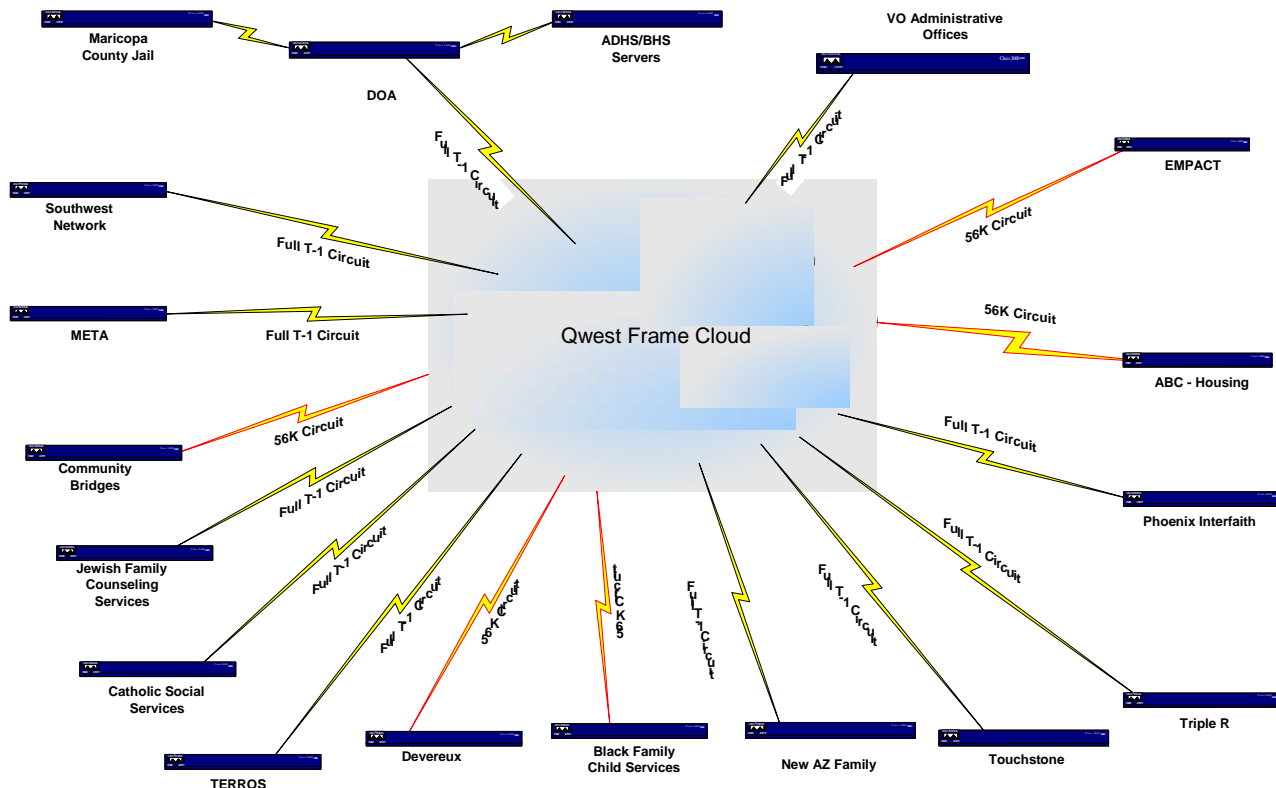
Network Architecture: Designed for Ultimate System Compatibility

Through the well-designed architecture of Local Area Networks (LANs), Metropolitan Area Networks (MANs) and an expansive Wide Area Network (WAN), we provide the foundation for compatibility.

With these networks, the Information Services Department is capable of providing an interface and/or data exchange with all provider and state systems. As the current RBHA, we conducted provider system surveys to obtain comprehensive information about providers' operating systems, software, personnel, and data management processes. ValueOptions used this information to help build the provider data exchanges; to implement transaction based triggers, to enable the submission of electronic enrollments and assessments prior to HIPAA, and to strengthen the foundation of the system as a whole.

Currently, ValueOptions provides electronic data exchanges with the following systems and providers. See the chart below for the latest electronic road map ValueOptions has created with its provider network.

Figure 5c.1 Network Architecture



Using state-of-the-art routers and switches, we offer a secure way for providers to connect and share resources with their RBHA, directly linking our main systems to provider systems. Through this network architecture, providers are able to securely enter the ValueOptions network and access resources including PRIDUS, AS400 mainframes, and several other applications that help them process and transfer data more easily. This network architecture is discussed in full detail in Section 5.d.

One way that we have used this network compatibility to enhance the coordination of care for consumers is by creating a link between META's Urgent Care Center information systems and ValueOptions clinical data. Jointly managing crisis care with META, ValueOptions believes that it was imperative that crisis staff had the ability to review background information when providing urgent care to consumers. Through our network, ValueOptions and META were able to come together and create a link between our systems to allow for Urgent Care clinical staff and ValueOptions case managers to view each others clinical information on each consumer—thus creating a means to rapidly coordinate appropriate care and to provide appropriate services.

Innovative Applications for Increased Compatibility

Using the ValueOptions network, we also provide several software and web-based applications that facilitate greater compatibility with our providers. These applications were created specifically by our Information Services team to help facilitate compatibility between ValueOptions and our providers, ensuring efficient and accurate data flow between providers and ValueOptions.

The ValueOptions Information Center (VIC) was one of the first major applications developed, and was the first step in creating the even more advanced systems that are now in use. Through VIC, providers could login via dial up system to upload files to ValueOptions, as well as to retrieve multiple data sets, allowing them to do a 100% audit of all data exchanges, including paid, pending or denied claims, enrollment status, and consumer assessment due dates.

Building on VIC, we created an even more innovative and user-friendly application—the Provider Reporting Information Download and Upload System, or PRIDUS (See Figure 5c.1). Instead of dialing into ValueOptions, providers can now access this Web-based system through any Internet connection. Besides allowing providers greater access to ValueOptions data, PRIDUS also offers enhanced security due to its built-in Secure Socket Layer (SSL), the highest protocol for web transactional security.

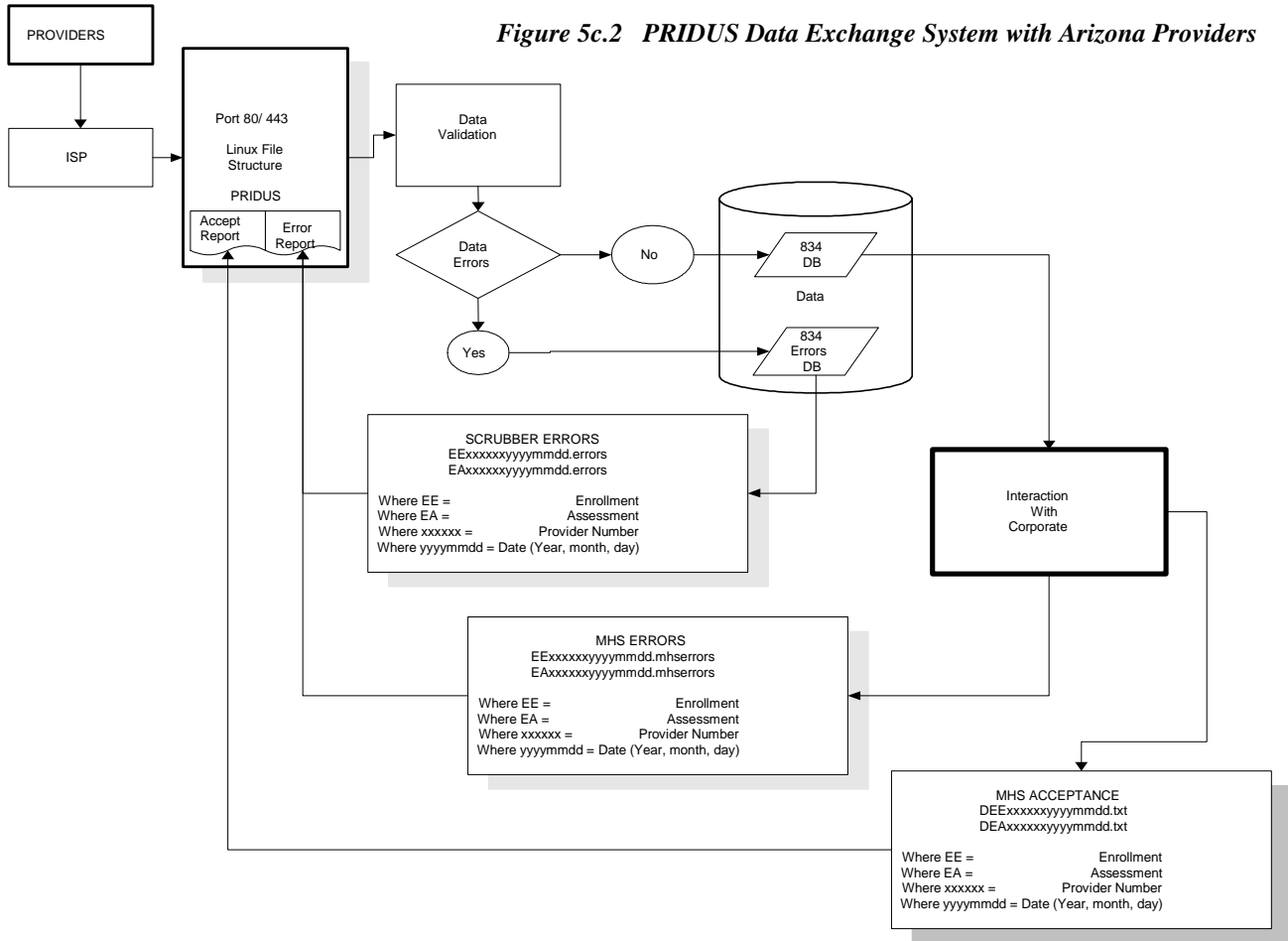
Before PRIDUS, 30% of enrollments and 27% of assessments were submitted electronically via VIC. The remainder of them were submitted as paper documents, which then had to be keyed in by ValueOptions staff. This processing required significantly more staffing resources than are now required for the submission of data. By the first quarter of 2004, we expect to have 80-100% of all forms submitted electronically through the PRIDUS application in a HIPAA compliant format.

Some of the features of PRIDUS are:

- online enrollment and assessment submission and processing,
- online claims submission,
- online provider referral log, allowing providers to electronically submit referral information, and
- automatically generated reports detailing claims status are paid, pending or denied.

By the first quarter of 2004, we have also scheduled to implement a capacity management feature, which will allow us to more effectively monitor and manage capacity and availability of space in inpatient facilities. As we continue to build on this system, we will be able to incorporate more system enhancements to further streamline and facilitate the Maricopa County Behavioral Health System's data management process.

Figure 5c.2 PRIDUS Data Exchange System with Arizona Providers



HIPAA Electronic Data Interface

With the implementation of new HIPAA standards, it is critical that we build compatible systems to ensure that ValueOptions and our providers are compliant with the new regulations. Although some larger providers have been able to program their software, or purchase HIPAA translators in order to comply with these new standards, many of the smaller providers in Maricopa County simply do not have the resources to purchase and maintain this expensive software. To help these providers become HIPAA compliant, we created an Electronic Data Interface (EDI) that providers can download at no cost. We currently offer EDI software for HIPAA professional and institutional claims transfer (837P and 837I). As a result of the initiatives, ValueOptions and all of Maricopa County providers are able to transmit data more seamlessly in a manner that ensures compliance with HIPAA.

Auditing Software

In order to successfully create compatible systems that can work together, it is critical to ensure that information is accurately submitted in a standardized format. Earlier data submission protocols were compromised by data entry errors. Thus, because of a typing error or a digit left off the social security number, forms were returned for correction and resubmittal. In 2002, we created a free software application for our providers allows them to audit or check the consumer enrollment and assessment information maintained electronically within their systems against ValueOptions edits. This software application allows providers to correct data errors prior to submitting to ValueOptions, and helps to improve the accuracy and integrity of enrollment and assessment data. Some large providers requested the source code, which ValueOptions provided to integrate these edits within their information systems. One particular large provider, Southwest Behavior Health Services, reduced data submission errors by over 90%. Another provider was able to submit over 1,000 late clinical assessments within a few days while maintaining a 99% error free rate.

Technical Assistance for Providers to Enhance System Compatibility

To maintain system compatibility, we often offer our Information Services technical services to our providers free of charge—helping with everything from reconfiguring their LAN, to providing technical training for their staff. Providers are also encouraged to call the ValueOptions help desk if they are having a computer glitch or need help with a technical issue. Frequently, we send a team of Information Services employees out to the provider site to provide technical assistance regarding individual compatibility and systems issues. In one case, when a provider's information system failed to operate correctly and the vendor was unable to make corrections, ValueOptions offered use of its own information systems free of charge to get the provider operational and to ensure continued consumer care and processing of claims data during the system failure. We strongly believe that sharing our technical resources with providers enhances the strength and viability of the overall behavioral health system.

As part of a basic decision support system, ValueOptions also supplies providers with automated reports to help them manage their business operations, including consumer liaison tracking, active user rosters, pharmacy management, fiscal management (including encounters and fee for service claims submission values against contract requirements), utilization information, and other management data.

Onsite Technical Support within ValueOptions

The final key to information systems compatibility is a strong Information Services team within the RBHA. Without a strong team, none of the above would be attainable. ValueOptions information systems are maintained at a high level by a diverse team of highly skilled technical experts. We maintain a permanent staff of Information Services professionals to improve and maintain the complete hardware infrastructure in place at our Arizona Service Center, including network, servers, telecommunications, Virtual Private Network (VPN), and desktop support. A trained and staffed Helpdesk, available to internal ValueOptions employees and providers, handles software/application support, while a full staff of Report Programmers, Application Programmers, Mainframe Programmers, Business Analysts, System Analysts and Database Administrators work to develop better ways to increase compatibility, system efficiency and overall service to our providers and ultimately to our consumers.

d. Network Configuration and Architecture

ValueOptions designed the physical network, Local Area Network (LAN), Wide Area Network (WAN), and Metropolitan Area Network (MAN) to not only support our current needs, but also to grow as the behavioral health system in Maricopa County grows. This network provides the foundational structure that allows us to offer an innovative new system interface with providers that not only helps them communicate, manage and transfer data, but also provides access to a wide array of data resources that ValueOptions offers. In essence, it allows providers to communicate effectively and securely and to have access to the information needed to better serve consumers.

To protect the data and to ensure reliable and timely data transfer, ValueOptions utilizes over 500 different network components, including routers, firewalls, switches, and an ATM backbone that can transfer 45 megabytes a second. Also included in this system are multiple T1 connection to providers and several state agencies, which allows data to travel at 100 times the speed of dial-up. All these components ensure that data goes to the right place as rapidly as possible, while maintaining the integrity of the data.

In addition, this state-of-the-art network is adaptable to quick changes, allowing traffic to be redirected in a mere fifteen minutes. This process is accomplished through the use of consistent, compatible hardware throughout the organization. By using layer three switching, we can accurately route information at faster speeds, once again contributing to the increased overall speed and productivity of the system. Operational processes run faster, making personnel more efficient and capable of doing more work in the same amount of time. In fact, the network could absorb a 300% increase in workload and see no degradation in performance.

The following section provides pertinent information regarding the network configuration and architecture for the Maricopa RBHA, including information regarding LAN connectivity for the Administrative Infrastructure located in Phoenix, as well as the WAN details for connectivity to the State of Arizona, local Providers, ValueOptions' Direct Service Sites and ValueOptions' Corporate offices. Following the narrative below is the supporting visual documentation (Figures 5d.1 through 5d.8.)

ValueOptions Arizona Service Center Connectivity to Direct Service Sites

The ValueOptions Arizona Service Center utilizes a Qwest DS3 45Mb ATM circuit at its hub, located in the Administrative Offices in Phoenix. There are 21 Direct Service Sites that connect to this hub location through Qwest 1.54Mb T1 frame-relay circuits. Located in the Main Distribution Facility (MDF) is the core router, a Cisco 3640, which terminates the ATM circuit and provides connectivity to our Direct Service Sites. The ValueOptions' Direct Service Sites use Cisco routers 2610, 2611XM, 2612 or 3620 to terminate their T1 frame-relay circuits. The Direct Service Sites use Cisco 2950 and 2924 switches for their local LAN connectivity (See figure 5d.6).

All computers are connected using Cat 5 UTP cabling throughout the individual infrastructures. Before we became the RBHA, the Direct Service Sites were only connected using a 56K dedicated data line. Since then we have upgraded these connections, allowing us to introduce new applications such as Outlook, which in turn facilitate greater communication between Direct Care Site staff and administration leadership. We have also introduced Internet capability to open a new avenue for research and web-based communication for clinical staff.

ValueOptions Arizona Service Center Connectivity to ADHS and Provider Agencies

Qwest also provides the necessary circuits that connect ValueOptions to the State of Arizona, as well as to 14 provider agencies (See figures 5d.1, 2 and 3). A Cisco 3620 router is used to terminate the Qwest 1.54Mb T1 circuit for the State of Arizona and these providers (See figure 5d.6). Prior to ValueOptions becoming the RBHA, there was no infrastructure in place to provide connectivity between the RBHA and its contracted providers. We currently provide connectivity to over 40 providers through frame relay, RAS, or VPN connections, with many more requesting this connectivity. This connectivity allows providers to have real-time enrollment and eligibility data. They are also able to access claims data, which enables them to better adjudicate their claims in a timely manner. All of these system enhancements allow providers to concentrate on providing care to their consumers by minimizing the resources needed to manage information flow.

ValueOptions Arizona Service Center Connectivity to Corporate Offices

The primary connection to the ValueOptions Corporate Office in Reston, Virginia is provided through a Sprint 1.54Mb T1 frame-relay circuit with a redundant 1.54Mb T1 backup frame-relay circuit to an alternate Corporate Office in Norfolk, Virginia. VPN is also used for additional redundancy to connect to the corporate offices in Virginia. Local network traffic intended for the corporate office is passed through an Expand compression device, which improves throughput by up to 400%. A Cisco 3640 router is used to terminate the T1 circuits, and a VPN backup circuit that connect to the Virginia corporate offices (See figure 5d.4). The introduction of the VPN backup allows for near seamless switchover in the event of a WAN outage. This process ensures the clinical staff is able to access the core business systems, which in turn allows for continued care to the consumers.

ValueOptions Arizona Service Center LAN Connectivity

The LAN configuration of the ValueOptions' administration building in Phoenix consists of an MDF and 7 Intermediate Distribution Facilities (IDF). The core switch is a Cisco 6509 with a Multi Layer Switch Feature Card (MSFC) for layer 3 switching. The Cisco 6509 switch supplies a Gigabit backbone as well as Gigabit LAN connections to our local Dell Servers. Both fiber and copper are used to supply the network with redundant connections throughout the administration building (See figure 5d.5, 8). Located in the 7 IDFs are 2 distribution layer Cisco 4506 switches, 13-access layer Cisco 2950 switches and 2 access layer Cisco 2950G switches. Internet connectivity is achieved through a 3Mb connection provided by Cox Communications. All traffic external to the network must pass through a Nokia Checkpoint firewall. A Cisco 3030 concentrator is used to terminate VPN sessions for remote connectivity into the ValueOptions network. Lastly there are two Intrusion Detection Systems (IDS) in place that monitor both the local network and the DMZ switch (See figure 5d.7).

Figure 5d.1 WAN Connectivity – All Entities High Level

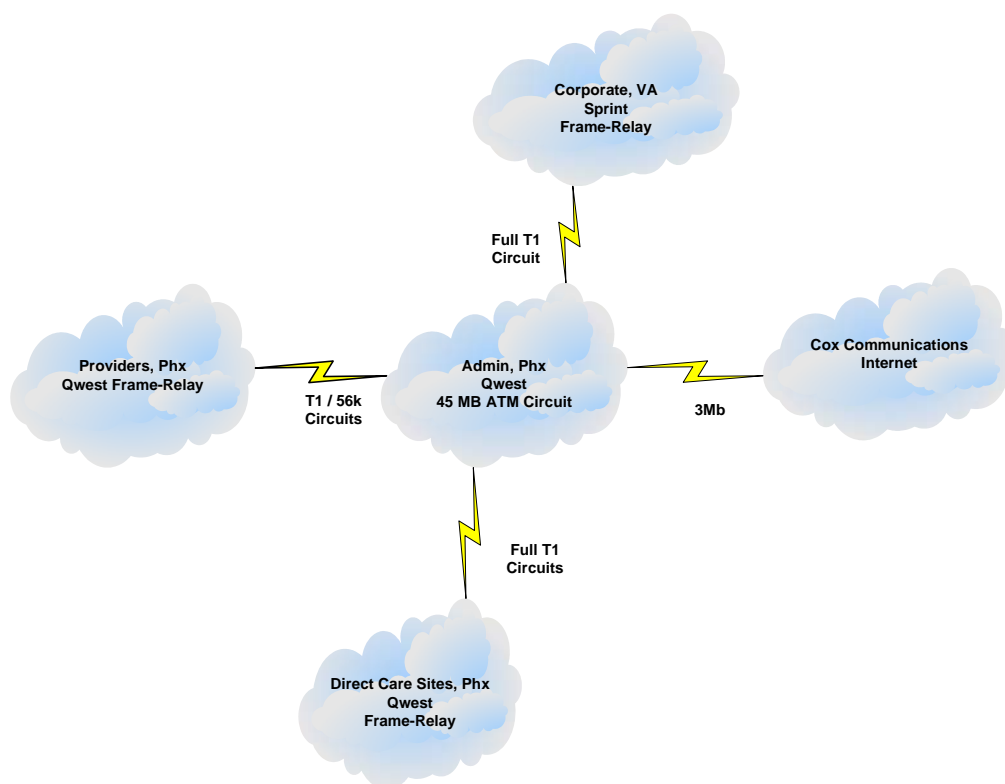


Figure 5d.2 Connectivity Between ValueOptions and Arizona Providers

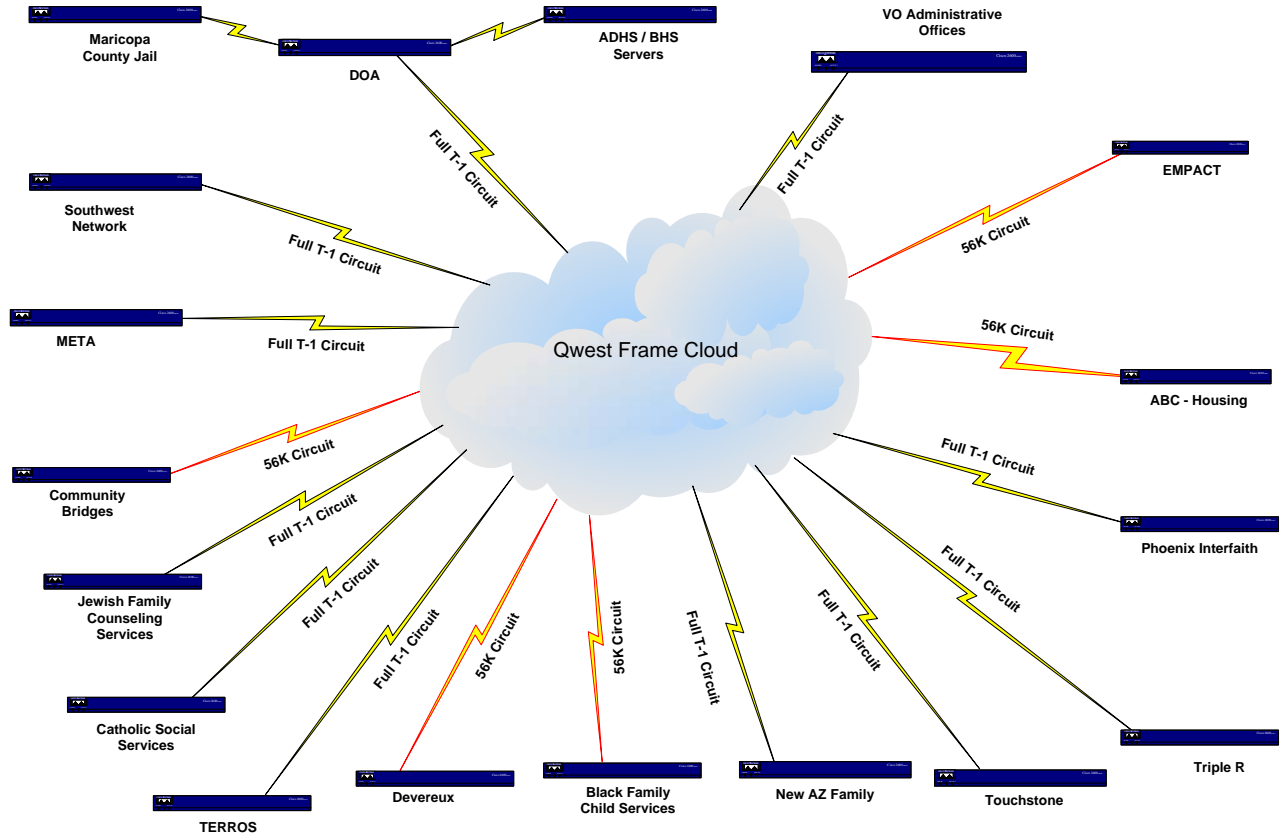


Figure 5d.3 ValueOptions Arizona Direct Care WAN Map – High Level
Identifies electronic connectivity between main administrative building and Direct Service Sites.

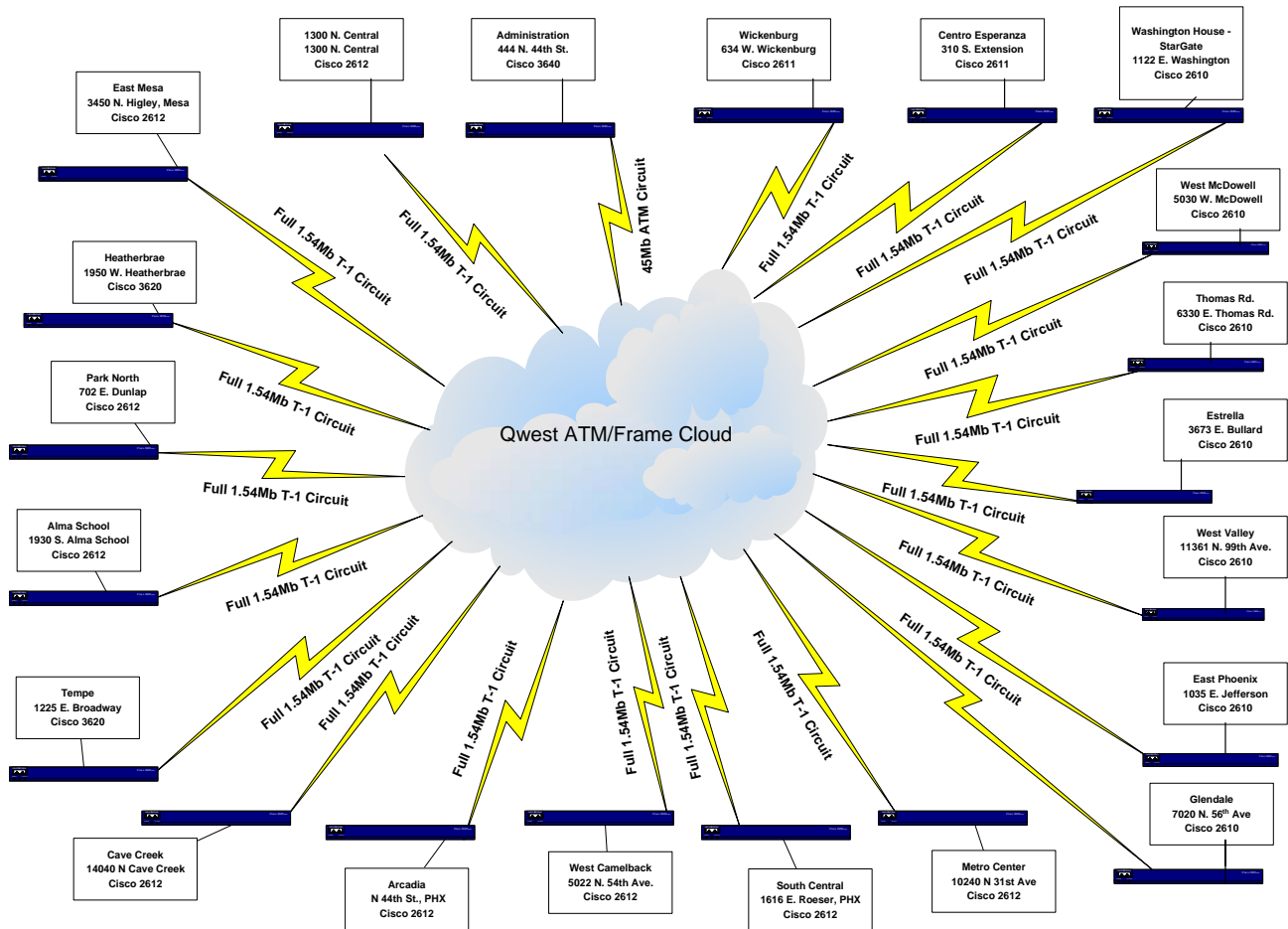


Figure 5d.4 Communications Equipment Between Administrative Site and Direct Service Sites

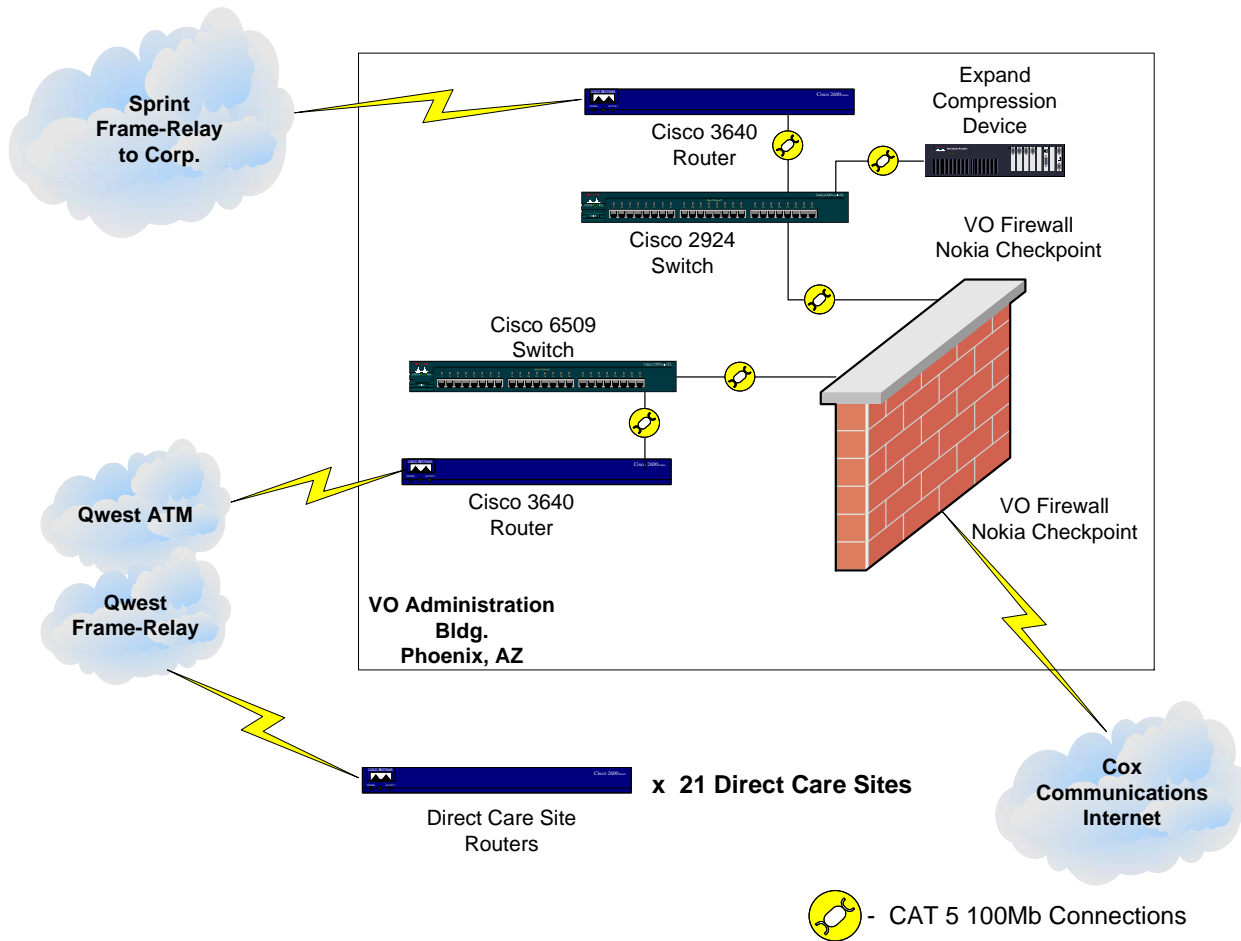


Figure 5d.5 Connectivity Between Internet Provider and ValueOptions Infrastructure

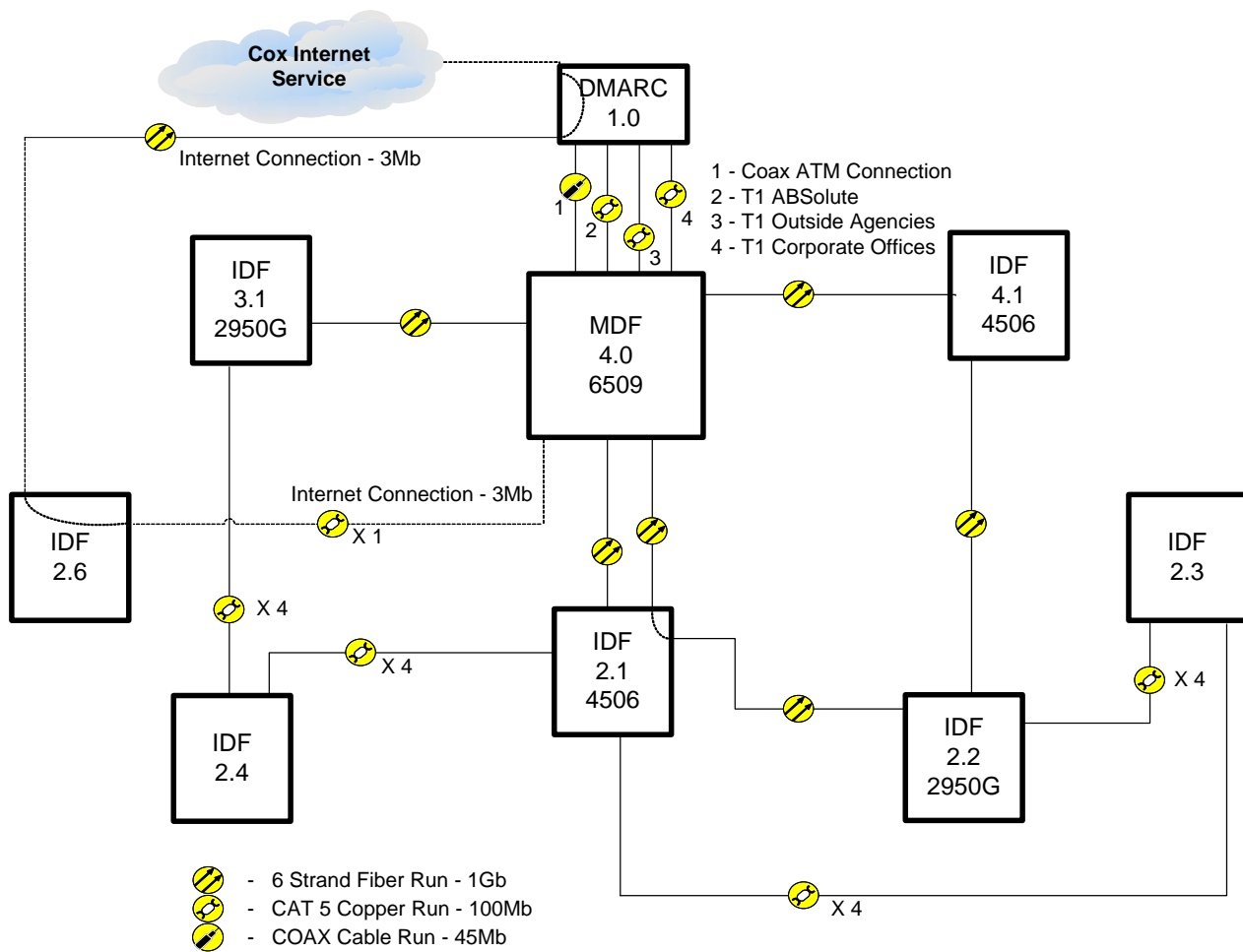


Figure 5d.6 High Level View of System Connectivity

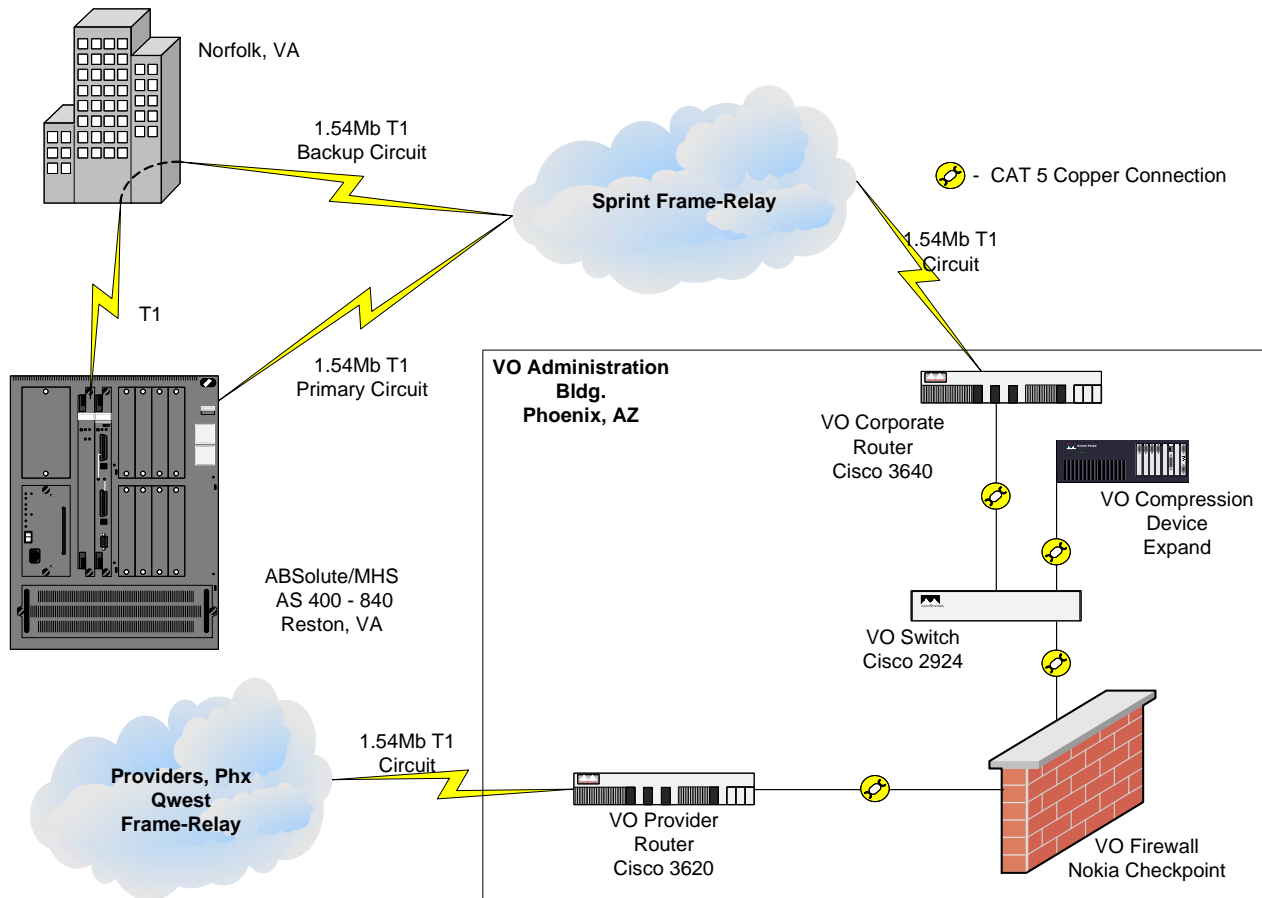


Figure 5d.7 High Level View of ValueOptions WAN Equipment and Connectivity

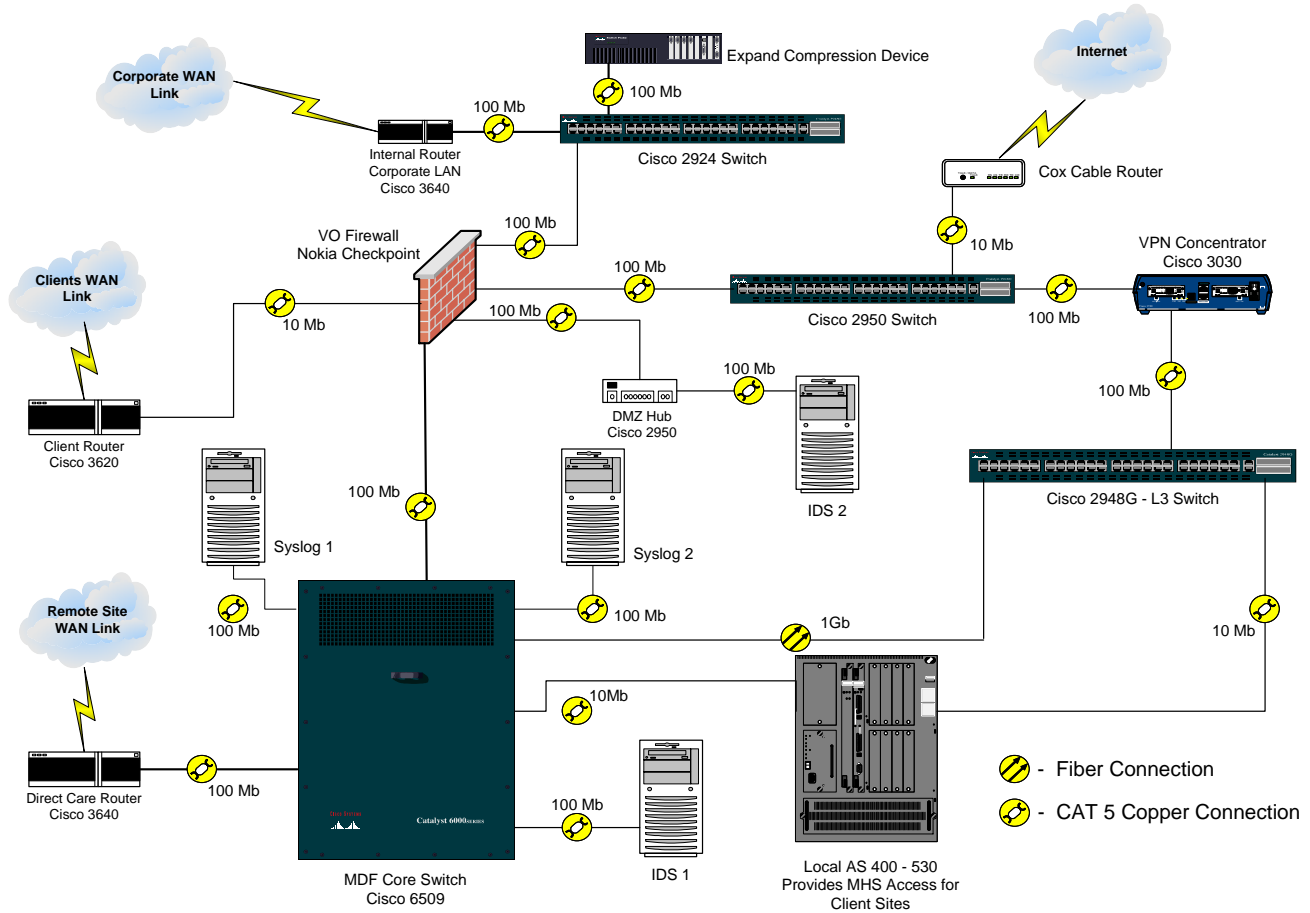
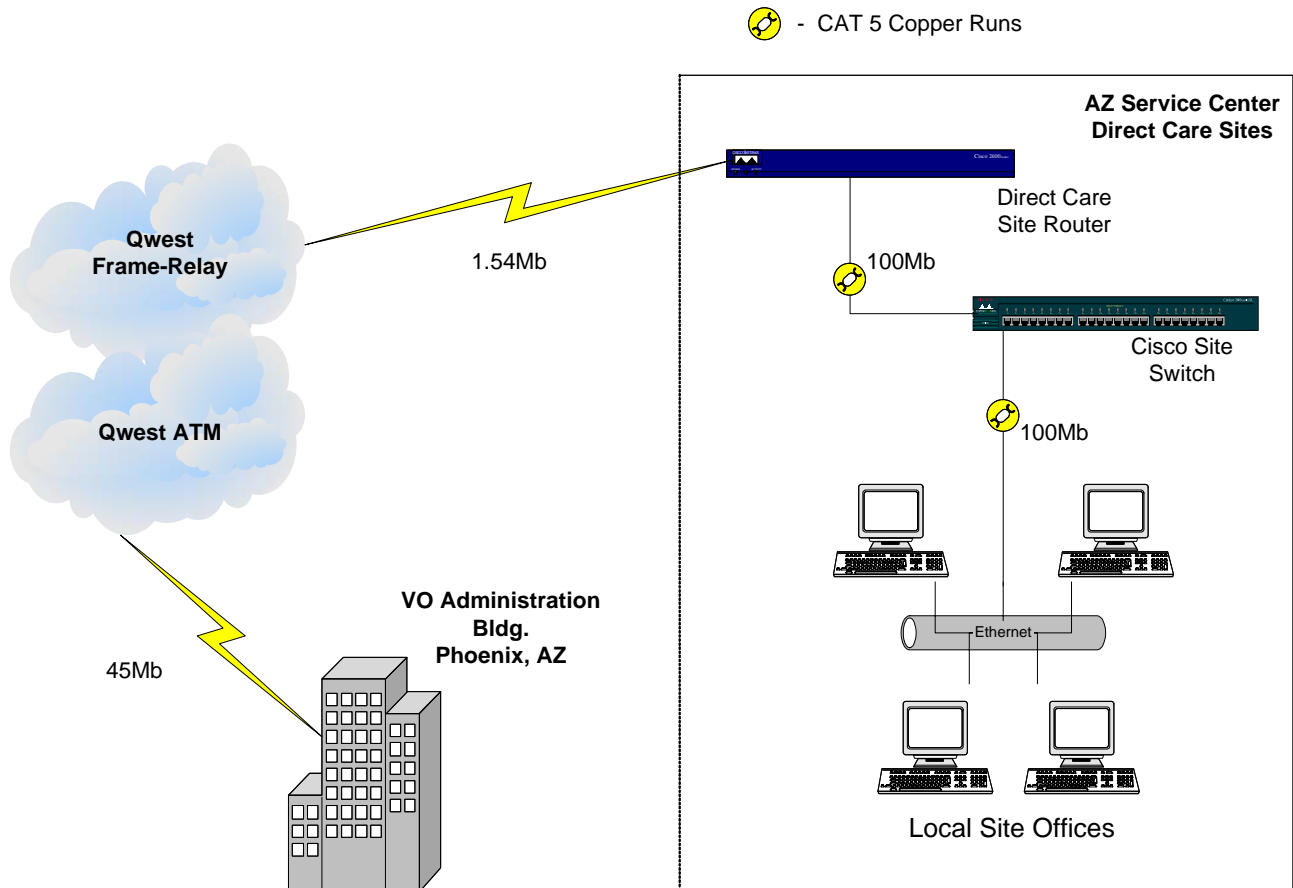


Figure 5d.8 High Level View of Vendor Connectivity to Administrative Office and Direct Service Sites



e. Ability to Provide an Electronic Data Interface

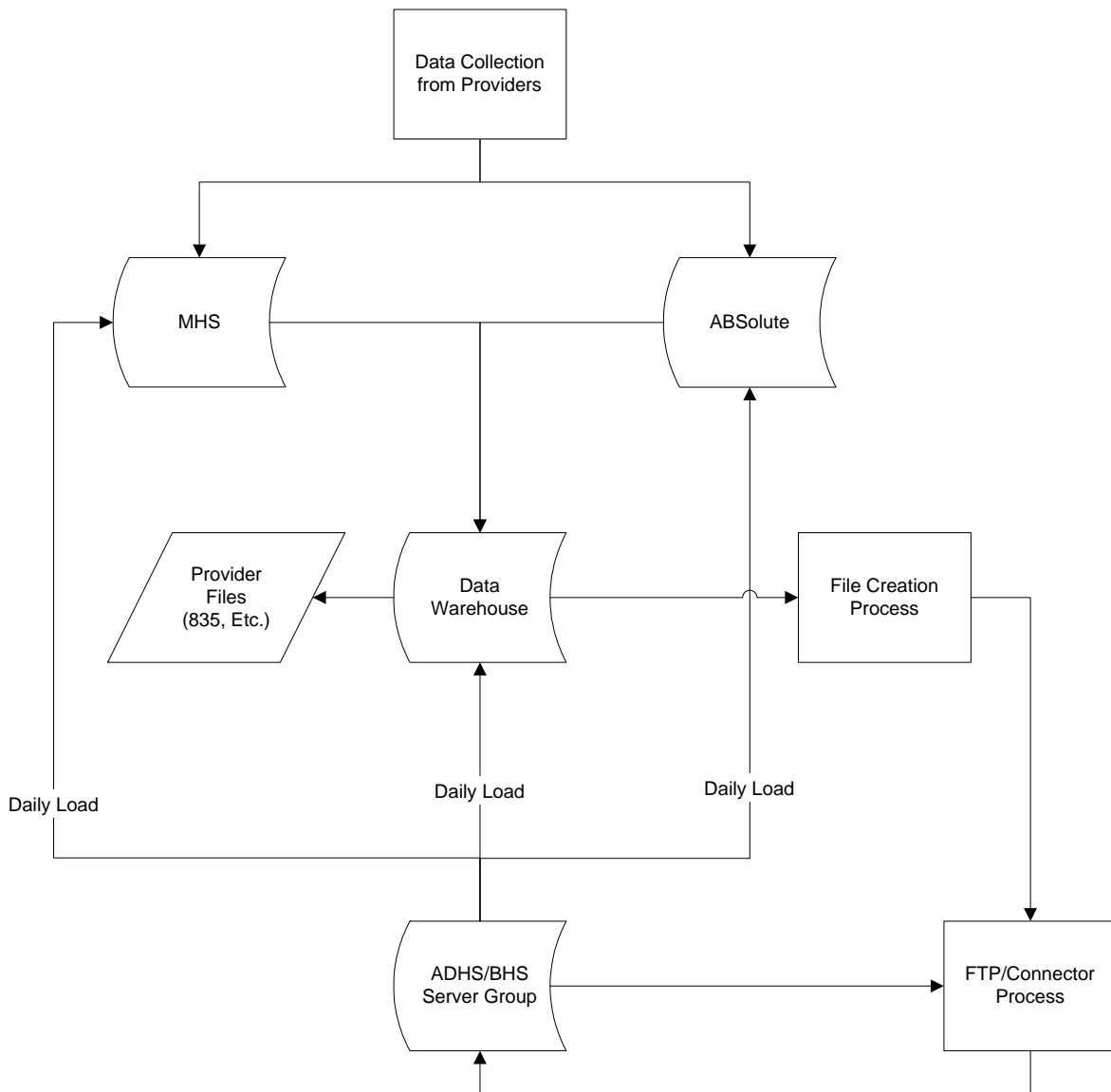
ValueOption's electronic data interface has been in place since January 1999. This interface allows ValueOptions to provide a reliable, efficient, and uniform process for transferring data. This is one of many examples showing how ValueOptions Information Services Department continues to make processes more efficient, allowing providers to focus on helping consumers rather than filling out paper work.

Going beyond the contractual requirements, our programmers created an easy-to-use Electronic Data Interface (EDI) application that automatically generates the HIPAA-compliant versions of required claim files and automatically transmits these files, directly to ValueOptions, providing time and taxpayer savings.

Providers can download this HIPAA compliant EDI program at no cost, offering a time-saving option for smaller providers who cannot afford the expensive HIPAA software that larger providers use. By offering an electronic format to those who would otherwise have to submit claims data via paper, we help eliminate substantial time from the process, thus enabling providers to submit claims faster and get paid faster. This process also saves the RBHA time and money that would have otherwise been spent on data entry and staff hours to manually enter the data.

In addition, we also maintain a backup system for the EDI, so that even if one line goes down we can handle the same job multiple ways. The following chart (Figure 5e.1) and file layouts illustrate the EDI that is used to serve the Maricopa County Behavioral Health Services Department and our consumers.

Figure 5e.1 High Level View of Electronic Data Exchange Interface Between ValueOptions and Arizona Providers



Data File Exchanged

The following tables detail the data exchange required within the CIS File Specification Layout Manual and ADHS/BHS Program Support Procedures Manual. All files are transmitted either daily, weekly, or monthly based on current requirements. The tables identify the current file name, whether the file is an outbound or inbound file, or if it is a miscellaneous file used for information purposes, and comments associated with the file.

*Please note that we have used the names of files within the CIS Manual for easy reference; however, since the printing of the CIS Manual, several have new names that are not reflected.

HIPAA 834 Intake Process

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
HINTKExx.hipaa	X			Original sent file
HINTKExx.error		X		Sent if Errors: Original file
HINTKExx.997		X		Sent if Errors: Error Reasons
UINTKExx.darbha			X	HINTKExx.darbha renamed for BHS internal use only
DINTDxx.dayyyymmdd.nn		X		Accepted Data
UINTKExx.ctyyymmdd.nn		X		Accepted Report File
UINTKExx.eryyyymmdd.nn		X		Unaccepted Data
UINTEDxx.eryyyymmdd.nn		X		Unaccepted Data

HIPAA 834 Closure Process

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
HCLSRExx.hipaa	X			Original sent file
HCLSRExx.error		X		Sent if Errors: Original file
HCLSRExx.997		X		Sent if Errors: Error Reasons
UCLSRExx.darbha			X	HCLSRExx.darbha renamed for BHS internal use only
DCLSSCxx.dayyyymmdd.nn		X		Accepted Data
UCLSRExx.ctyyymmdd.nn		X		Accepted Report File
UCLSRExx.eryyyymmdd.nn		X		Unaccepted Data

HIPAA NCPDP Encounter Drug Processing

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
hendrg08.hipaa	X			Original sent file
HDRGxx.error		X		Sent if Errors: Original file
UENDRGxx.darbha			X	HDRGxx.darbha renamed for BHS internal use only
DENCDxx.dayyyymmdd.nn		X		Accepted Data
H74-ENC-RPTxx.yyyymmdd.nn		X		Accepted Report File
UENDRGxx.eryyyymmdd.nn		X		Unaccepted Data

HIPAA 837P Encounter HCFA Processing

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
henmed08.hipaa	X			Original sent file
Henmed08.error		X		Sent if Errors: Original file
Henmed.997		X		Sent if Errors: Error Reasons
UENMEDxx.darbha			X	HMEDxx.darbha renamed for BHS internal use only
DENCDxx.dayyyyymmdd.nn		X		Accepted Data
UENCTRxx.ctyyyymmdd.nn		X		Accepted Report File
H74-ENC-RPTxx.yyyymmdd.nn		X		Accepted Report File
UENCTRxx.eryyyymmdd.nn		X		Unaccepted Data

HIPAA 837I Encounter UB Processing

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
HenINPxx.hipaa	X			Original sent file
HenINPxx.error		X		Sent if Errors: Original file
HenINPxx.997		X		Sent if Errors: Error Reasons
UENINPxx.darbha			X	HINPxx.darbha renamed for BHS internal use only
DENCDxx.dayyyyymmdd.nn		X		Accepted Data
UENCTRxx.ctyyyymmdd.nn		X		Accepted Report File
H74-ENC-RPTxx.yyyymmdd.nn		X		Accepted Report File
UENCTRxx.eryyyymmdd.nn		X		Unaccepted Data

Encounter Errors: Download from DBHS

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
ECERR.TXT				
ECERR.TXT.CCYMMDD		X		Encounter Error Code File
ECERRFLD.TXT				
ECERRFLD.TXT.CCYMMDD		X		Encounter Field File
ECFLD.TXT				
EDFLD.TXT.CCYMMDD		X		Encounter Error CorrectionFields File

Demographics

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
ddmogxx.daccyyymmdd.nn		X		Demographic Download File
h74248xx.outccyyymmdd		X		Demographic Resync File. From CIS
Udemogxx.ercyyymmdd.nn		X		Demographic Download Error File
udemog08.darbha	X			Demographic Upload File

Miscellaneous

Filename	Outbound To BHS	Inbound To VO	Misc	Comments
refer01.ZIP		X		Reference 01 File. AHCCCS via DBHS
refer02.ZIP		X		Reference 02 File. AHCCCS via DBHS
yymmdd FTPXX222 M		X		Service Authorization Resync File. On demand DBHS
h74tpl.yymmdd		X		Third Party Liability Consumer Information. AHCCCS via DBHS/CIS
capfleccyymmdd.ZIP				
h74capfile.txt		X		Capitation File. AHCCCS via DBHS
h74capwh.xx.yyyy.ccyymm		X		RBHA Capitation Extract File. DBHS
ddwnldxx.ctccyymmdd.nn		X		Download Report File. DBHS
drostinc.ctccyymmdd.nn		X		Daily Enrollment Report. DBHS
h74445f.ctccyymmdd		X		Weekly Enrollment Report. DBHS
dahcdxx.daccyymmdd.nn		X		AHCCCS Eligibility File. DBHS
yymmdd FTPXX247 M		X		AHCCCS Eligibility Resync File. DBHS on demand
u640rsp.yyyymmdd		X		Daily Response File. AHCCCS via DBHS
u640par.yyyymmdd		X		Daily Response Partial Match File. AHCCCS via DBMS
U640dds.yyyymmdd		X		Daily Response Demographic Discrepancy. AHCCCS via DBHS
U640adr.yyyymmdd		X		Daily Address Change File. AHCCCS via DBHS
u640hpc.yyyymmdd		X		Daily Health Plan Change File. AHCCCS via DBHS
Drostful.daccyymmdd.nn				
drostinc.ccyymmdd.nn				
drostful.ZIPccyymmdd.ZIP		X		Enrollment Roster File. DBHS
Daxxixx.daccyymmdd		X		DAXXI KidsCare File. DBHS
Yymmdd.ltc		X		ALTCS Long Term Care Consumer Info Extract.DBHS
Fyifle.ccyymmdd		X		Medicare HMO Matching Eligibility. AHCCCS via DBHS
profile.ZIP		X		Provider File. AHCCCS via DBHS
yymmdd FTPXX227 M		X		Provider Resync File. DBHS on demand
Provider.ZIP		X		Provider Profile File. DBHS
rm90m639.yymmdd		X		Recipient Counts Report. DBHS. Generated by AHCCCS

Software used to create each file is based on the location where it originates. When files are produced within ABSolute they are created with Advantage 2E, files produced from MHS are created using COBOL, and files produced from our data warehouse are created using SQL and Crystal Reports. All files pulled in from ADHS/BHS are loaded into the systems using the same software, respectively.

f. System Downtime and Change Management Process

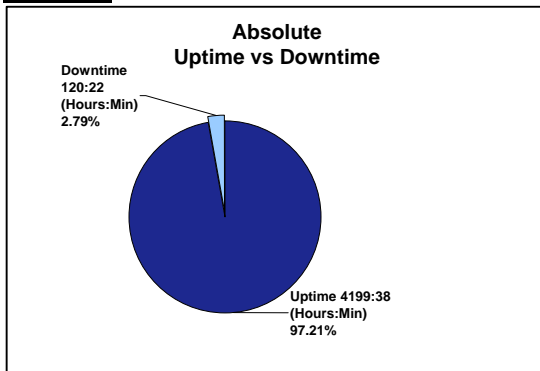
Maintaining a stable and reliable production system is critical to the success of business operations in all industries, especially when providing and managing a complex service system such as behavioral healthcare. The Arizona ValueOptions Service Center, in conjunction with the ValueOptions Corporate Center in Virginia, continually strives to build and maintain solid and reliable business networks and systems.

Through these efforts, we have implemented a system that exceeds industry standards in regards to system uptime. In fact, in the five years we have managed the Arizona Service Center, the business systems have never been completely down, except for scheduled downtime for maintenance. For providers, and the Department of Behavioral Health Services, this means that they have a reliable system of communication, data transfer and management that they can depend on to help them do their job efficiently.

The system and network analysis information outlined below demonstrates this dedication to providing top quality business systems to ValueOptions consumers, providers, and employees. This information describes systems availability over the past six months. Following the Downtime Analysis is information regarding policies and procedures for programming changes and parallel systems.

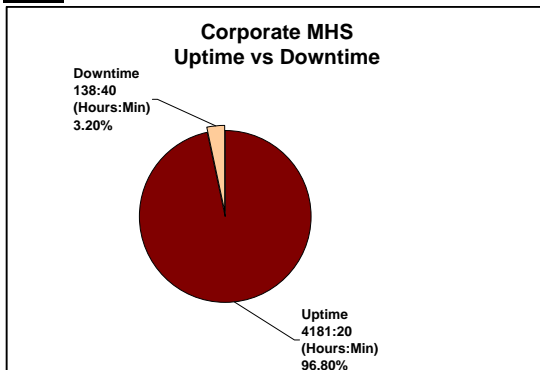
Uptime vs. Downtime Analysis - Business Systems

ABSolute



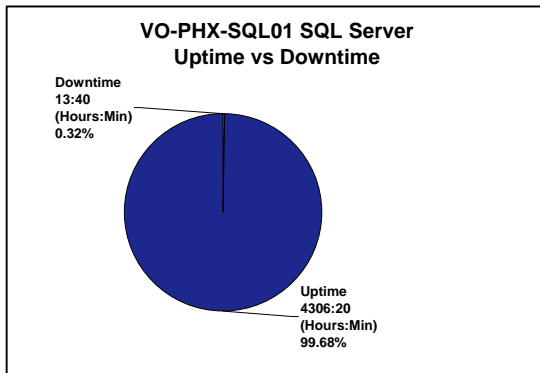
The ABSolute system is our main Direct Care Consumer Record system. Tracking over the last six month identifies 120 hours and 22 minutes of downtime (2.79%) caused by WAN/LAN disturbances, emergency system repairs, scheduled maintenance or downtimes that run longer than scheduled. Uptime of the system was 4,199 hours and 38 minutes (97.21%).

MHS



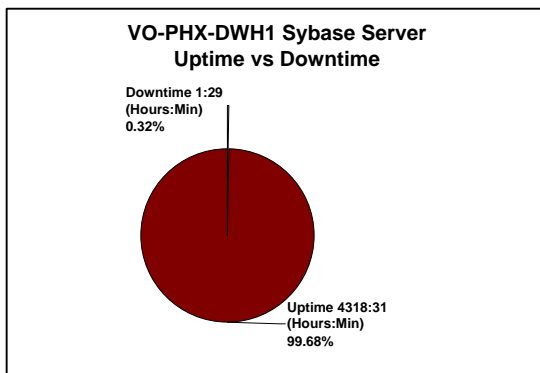
The MHS system is ValueOptions' main operational system and direct interface device for providing core information to ADHS/ DBHS. System downtime for the past 6 months was 138 hours and 40 minutes (3.20%) for scheduled and unscheduled maintenance. Uptime of the system was 4,181 hours and 20 minutes (96.80%).

VO-PHXSQL01 – Local SQL Data Warehouse



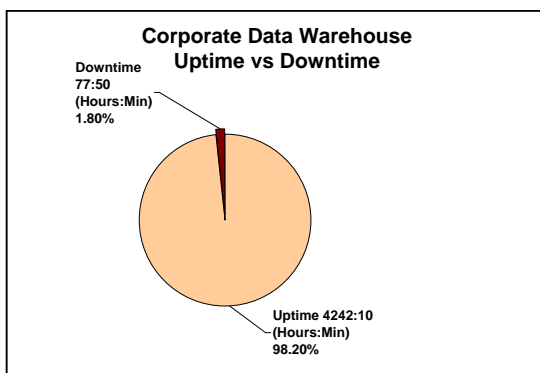
The data warehousing system for the Arizona Service Center is made up of two individual systems; a Microsoft Enterprise Edition SQL 2000 Server and a Sybase 11.9 Sever. The SQL Servers unscheduled down time was 13 hours and 40 minutes (0.32%). Downtimes are caused by WAN/LAN disturbances, emergency system repairs, or scheduled maintenance. Uptime was 4,306 hours and 20 minutes (99.68%).

VO-PHX-DWH1 – Sybase Data Repository



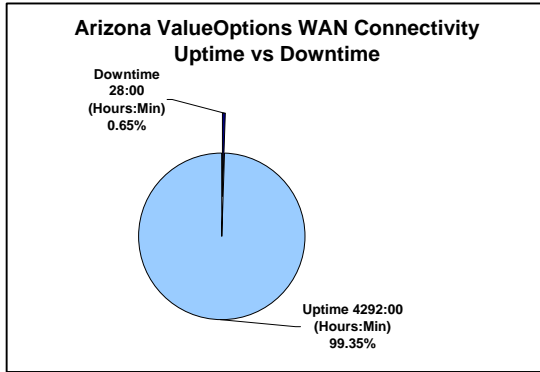
The Sybase Server is the redundant data source and has experienced minimal downtime in the last six months totaling 1 hour and 29 minutes (0.32%) vs. 4,318 hours, and 31 minutes (99.68%) uptime. The SQL 2000 Server and the Sybase Server maintain the data where 80% of our required reporting under the current contract is produced. Downtimes are the result of WAN/LAN disturbances, emergency system repairs, or scheduled maintenance.

Corporate Office (VA) Data Warehouse



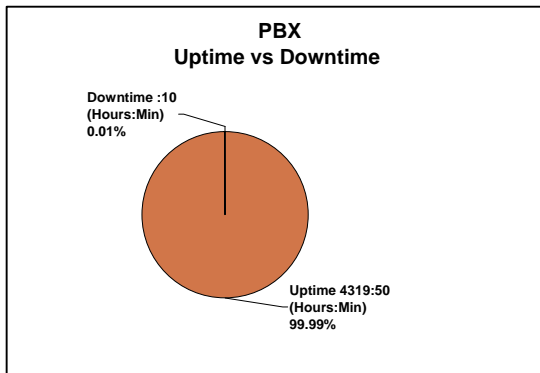
The Corporate Data Warehouse is the primary repository for all data stored and processed on the MHS system, and is used as a distribution system for all ValueOptions contracts. During the past 6 months this system had a total of 77 hours and 50 minutes (1.80%) of downtime due to emergency system repairs, scheduled and unscheduled maintenance or LAN/WAN Disturbances. Uptime was recorded at 4,242 hours and 10 minutes (98.20%).

Uptime vs. Downtime Analysis - WAN



The Arizona ValueOptions WAN connection to our Corporate Offices in Norfolk, Virginia serves as our main connection to our remote business systems. The WAN downtime over the past six months was 28 hours (0.65%). The WAN uptime during the past six months was 4,292 hours (99.35%). Downtime can be attributed to scheduled and unscheduled maintenance and carrier issues.

Uptime vs. Downtime Analysis – PBX and Queued Calls



The Meridian 1, Option 61C PBX telecommunications system is utilized by clinical and non-clinical staff to provide quality service to ValueOptions' providers and consumers. During the past 6 months this system experienced a downtime of 10 minutes (0.01%) for scheduled system upgrades. System uptime for this period was 4,319 hours and 50 minutes (99.99%).

ValueOptions Change Management Process

ValueOptions defines Change Management Process (CMP), previously described in Volume 5.b and summarized here, as the process that governs changes related to the development of new systems, enhancements made to existing systems, and technical support. ValueOptions CMP objective is to ensure that a standardized, effective, and efficient process is in place for the intake, approval, prioritization and fulfillment of requests for service received by the Arizona ValueOptions Service Center Information Services Department. The CMP controls, prioritizes, and streamlines the delivery of changes to our information technology products and services. This process covers nine primary phases, which are; Request Initiation, Business Support Analysis, Project Approval and Design, Operations Request, Development/Change Control, Testing and Acceptance, Training and Documentation, Release and Post Release.

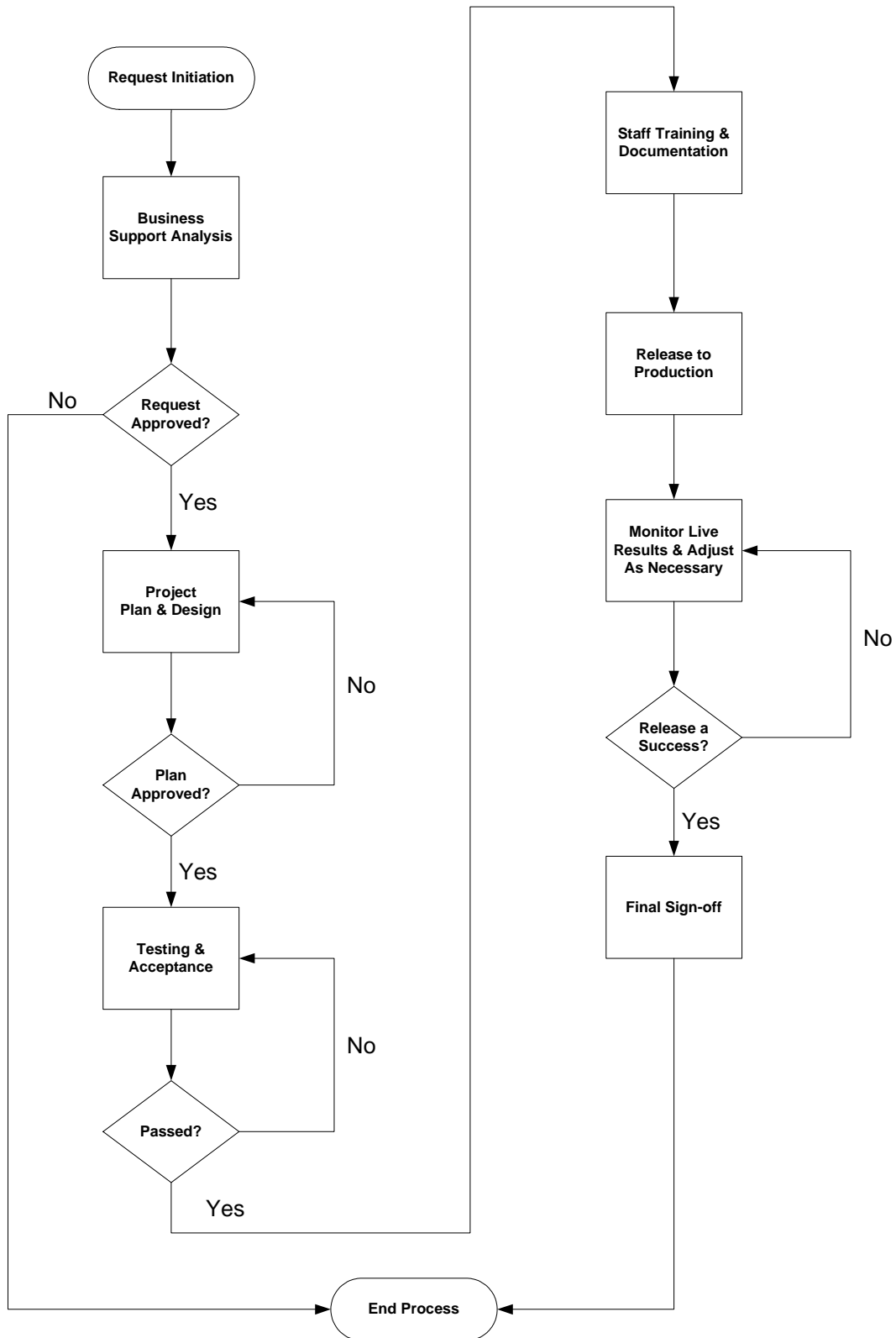
The first phases of the CMP cover the receipt of requests from the user community, the process of analyzing the request for business need, impact and benefit, the merit of the request, the escalation of the request to project planning, design, and approval phases. Once approved, the project proceeds to the development and testing phase.

The Development and Testing phase proceeds through three levels of testing. In Level 1 Testing, the programmer completes unit testing and checks for reasonable results. The modified modules are moved to locations that permit integrated testing. In Level 2 Testing, an integrated test is performed to check that the modifications are compatible with other components of the application or with external system interfaces. Level 3 Testing involves User Acceptance testing. The users test the modifications using applicable business processes. This level of testing ensures that the modifications do not detract from system functionality and the application will perform successfully under realistic business environments. Issues are logged and categorized on a Test Phase Issue List, and then reviewed by the project team.

During these phases, hardware and/or system projects are carried out in testing labs on non-production systems to verify results prior to release into the production environment. With regard to programming changes, these too are carried out on development servers in a parallel non-production environment.

Once all changes or upgrades have been completed and properly tested, affected personnel are given the necessary training and/or documentation to support the changes and a release date is set. All affected departments and/or personnel are notified of any anticipated outages or issues that may arise from the release of the new systems or programs including contact information for anyone experiencing any post release issues. Once the release has been completed, the technical staff monitors the performance of the affected systems as well as surrounding systems to ensure compatibility with existing systems and assess the success or failure of the move to production. The following chart, Figure 5f.1, represents a summarization of the flow as it relates to Change Management.

Figure 5f.1 Summarization of Change Management Process



g. IT Personnel Training

In today's rapidly changing Information Technology environment, keeping Information Services employees well trained and knowledgeable about the latest technological developments and capabilities is critical. More importantly the staff must understand how these new developments fit into the established processes, operations and vision of the organization as a whole.

Our Philosophy

In the ValueOptions Information Services Department, we look at training holistically, and thus our philosophy revolves around not only keeping each employee well trained in their particular area of expertise, but also ensuring that all employees understand how the rest of the organization works and how their contributions affect the entire service center. The same understanding is needed regarding the affiliates we work with, including providers, other state agencies, and consumers. In the end, we must have a staff that understands how his or her job directly influences the level of care that each consumer receives.

We accomplish this education through cross training. Through a system of advanced technical training, combined with operational training to help our staff understand how each area of managed behavioral healthcare works within the system, our staff is able to develop more efficient ways to manage, organize, process, transfer and protect information.

How Cross Training Works

Each part of our cross-training system contributes to the long-term growth and success of Maricopa County's behavioral health system. Through operational training, the Information Services team becomes aware of issues that affect the system as a whole, while technical training gives them a multitude of tools and skills to address these issues and come up with solutions to help the system run more smoothly.

On the operational side of our cross-training system, Information Services Business Analysts work with other departments within the organization, as well as with our affiliates and other state agencies, to understand and document each group's operational processes. Our Business Analysts then create operational process flow charts and train other Information Services employees to help our team understand how each part of the behavioral health system works. Through this training, the Information Services team can see and identify areas of the system that are in need of streamlining, and can apply their expertise to help the system become more efficient.

On the technical side, our cross training system provides access to advanced training resources such as workshops, seminars, college courses and other continuing education. External technical training enhances the current technical skills and brings new skills into the Information Services department. These courses give Information Services employees the knowledge to improve the performance, reliability and integrity of data. Information Services employees have also gained new skills in the area of security to comply with HIPAA and in the development of new, more powerful applications. This technical training has helped us create a skilled and diversified Information Services team that is a model for service centers across the country and for other RBHAs within Arizona.

In addition, what makes our cross training unique is the fact that it capitalizes on the skills of each Information Services employee to help train others and make the group stronger as a whole. Each employee is encouraged to share his/her knowledge and to train others in areas of special expertise. This part of cross training ensures business continuity, providing assurance that even if one person in our team is unable to perform their job, the Information Services department would still be able to perform their duties.

New Employee Training

Cross training starts the day an employee is hired. It begins with a series of standardized training courses to orient the employee to the company and to the behavioral health system. This training includes everything from details on the Arnold vs. Sarn Lawsuit to HIPAA standards and cultural competency. Then, each new employee is assessed by their immediate manager to determine the individual training needed to perform their core job duties. For a programmer, this could include technical classes, as well as clinical system classes to understand the scope of work performed in the main systems.

How Cross Training Benefits the Behavioral Health Care System

Technical Training

Many of the past innovations, and continuing improvements to the behavioral health management information system came about as a direct result of cross training. From applications that improve the processing on the AS400 systems to web-based interfaces for improved communication with the providers, the technical training we provide for our employees has paid for itself many times over by giving our employees the skills to develop and implement services and applications that make the behavioral health system more efficient. This technical training will continue to pay off as we roll out more web-based applications to enable data interchange between providers and ValueOptions. With new technology and continued technical training, we will be able to automate more and more services, decreasing the margin for error and creating a more efficient and cost-effective system.

Security Training

As a result of offering Certified Information Systems Security Professional (CISSP) training to selected employees as a part of our advanced technical training, the ValueOptions Information Services department now has two internationally certified security professionals. With this training we have already developed and implemented an application development methodology that ensures the security of confidential consumer information. Also, with HIPAA security compliance coming into effect in the near future, this security training will allow us to ensure that our organization and our providers are compliant with new legislation.

Operational Training

The operational side of our cross-training system has also directly benefited the Maricopa County behavioral health system. As Information Services employees are trained on internal operational processes, they develop a deeper understanding of how their own job duties fit into the whole process and are often able to find ways to make the overall system even more efficient. For example, when one of our programmers was trained on how claims processing works, he was able to see how his programming capabilities could help streamline the claims processing operation. As a result of the training, a software application was designed that allows thousands of claims to be processed in just a few hours, instead of the days or weeks it used to take to process the claims manually. By automating this system, claims are processed more accurately, saving time, energy and money.

Community Contributions

With the extensive technical skills our Information Services employees have developed through this training, ValueOptions has been able to offer technical support and training for the providers in the Maricopa County network. This includes one-on-one training and technical assistance, as well as group trainings. These collaborative relationships will continue in the future as the MIS department continues to look for ways to strengthen communications and data transmission with providers.

Types of Training Available

ValueOptions offers training in many forms including group seminars, workshops, one-on-one tutorials and college courses. Each year, employees are given a stipend for professional development at colleges and universities. Since Information Services employees are allowed flextime, they are able to work around their class schedule, ensuring they are able to complete their degree program. We currently have people working on Associate degrees, Bachelor degrees, Master's degrees, and PhD's.

In addition, ValueOptions Information Services department has developed an innovative, easy to use online Computer Based Training (CBT) application. Through the ValueOptions Intranet, our Information Services employees, as well as other employees, can log on and complete the training they need right on their computer, allowing them to work at their own pace and within the timeframe that works best with their schedule. At the end of each online course, employees complete a test and the results are tracked. This application not only ensures that accurate, standardized information is disseminated throughout the organization, but also decreases the staff resources needed for training.

The following is a list of courses the Information Services team has completed:

VO Internal HR Training

Manager Training
Ethics
Sexual Harassment
HIPAA Privacy
Selection and Interviewing Prospective Employees
Performance and Appraisal
Leadership Goals and Outcomes
Correcting Performance Problems
Giving and Receiving Constructive Feedback

Clinical System Training

ABSolute Case Management
ABSolute Scheduling and Billing
ABSolute Site Management
ABSolute Affiliation
ABSolute Operations
Composition and responsibilities of a clinical team
Living with schizophrenia and other mental illnesses
Crisis System Overview
Managed Care
Cultural Competency
Adult Assessment Tools
Coding and Billing
Court Ordered Treatment
Housing
ALTCS Overview
Access to Care
Case Management
Scheduling
Bioinformatics

Mainframe Courses

Beginning AS/400 Operations
Intermediate AS/400 Operations
Intermediate AS/400 Query

Office Products

Microsoft Visio
Microsoft Project
Microsoft Outlook
Microsoft Word 2002 Level 1
Microsoft Excel 2002 Level 1
Microsoft Excel 2002 Level 2
Microsoft PowerPoint 2002 Level 1
Microsoft PowerPoint 2002 Level 2

Hardware

CompTia A+ Certification Training
FLUKE certification

Telecomm

Northern Telecom Norstar Phone system
Northern Telecom NAM Voice mail
Northern Telecom Option 61 Phone System
Northern Telecom Meridian Max
Northern Telecom CCR
Northern Telecom Meridian Voice mail
Verint Voice recorder
BICSI communication wiring standards
Meridian PBX and Norstar phone systems

Operating Systems & Networking

Microsoft Windows NT Workstation 4.0
Microsoft Windows NT Server 4.0
Microsoft Networking Essentials
Microsoft Windows NT Server Enterprise
Microsoft Exchange Server 5.5
Microsoft Exchange 2000
Microsoft SQL Server 2000
Microsoft SQL Server 7.0
Microsoft 2000 Professional
Microsoft 2000 Server
Microsoft Network Infrastructure
Microsoft Active Directory
Microsoft Windows XP
Cisco Networking
Windows 98
Implementing and supporting NT Workstation
Implementing and supporting NT Server
Implementing and supporting NT sever in the Enterprise
Internetworking with Microsoft TCP/IP on Microsoft Windows NT 4.0
Microsoft TCP/IP
Novel 5.5

Database

Microsoft SQL 2000 Programming
Microsoft SQL Server 2000 Administration
Oracle 8 DBA Certification
Microsoft SQL 2000 Performance tweaking
How to use stored procedure effectively in Sybase 11
Administering Microsoft SQL Server 7.0
Designing & Implementing Databases using MS SQL Server 7.0"
Sybase 11.5 Administration
Microsoft Access 97 & 2000

Programming Language

UML (Universal Modeling Language)
Visual Basic 6.0
PHP Programming
PHP web based scripting
JavaScript Complete
TSQL Programming
Visual Basic .NET
Visual C# .NET
XML Software Analysis & Design
JWalk training at Seagull in Atlanta, GA
Intro to HTML, Intermediate HTML
Dreamweaver Introduction
Intro to Fireworks
MapInfo
Crystal Report 7.0 Beginning and Intermediate
Visual Basic 5.0
ASP.NET
UML (Unified Modeling Language)
System Analysis and Design
Database Design methods (relational databases)
Best practices in Software construction

Project Management

Project Management Certificate programs at the University of Phoenix
PMP Training (Project Management Professional)
Microsoft Project 2000 Training

Security

Certified Information Systems Security Professional (CISSP)
Comdex Security Courses
Arizona Computer Info Expo

Certifications held by ValueOptions of Arizona MIS employees

CISSP (Certified Information System Security Professional)
MCSE (Microsoft Certified Systems Engineer) (NT 4.0 & Windows 2000)
MCSA 2000 (Microsoft Certified Systems Administrator)
MCP (Microsoft Certified Professional)
CCNA (Cisco Certified Network Associate)
CCNP (Cisco Certified Network Professional)
OSDN (Open Source Developers Network)
LCP (Linux Certified Professional)
Network Plus
COMPTia A+ Hardware and Software Certification

h. System Data Archive and Retrieval

ValueOptions' management, and the Information Services team understand the importance of thinking proactively to anticipate possible problems in today's business world. In order to ensure uninterrupted service in disaster or emergency situations, we have developed a comprehensive data archive and retrieval system as part of our comprehensive Disaster Recovery/Business Continuity Plan.

Our Current Configuration

A redundant site at our corporate location in Virginia, in conjunction with local backup servers, hardware and over 23 warm sites in Maricopa County, ensure business continuity. The ValueOptions Arizona Service Center already has a data archival and retrieval system in place that exceeds most industry standards. We are committed to providing reliable service not only to our own internal staff but also to all of those who depend on our systems, including providers, networks, and the Department of Behavioral Health Services.

Plans for the Future

ValueOptions is currently implementing a plan to upgrade our systems to the highest possible industry standards, with completion scheduled for mid-2004. This extensive "gold standard project", with over five tiers of redundancy, is designed to further enhance existing archival and retrieval systems in order to ensure the safety, integrity and availability of ValueOptions information systems under almost any foreseeable adverse situation.

The following pages describe the current backup and retrieval system for ValueOptions Information Systems data, including the specific hardware and a summary of our Disaster Recovery/Business Continuity plan. Also included are our plans for upgrading the system in the near future.

Maricopa County RBHA Administrative Offices

Disaster Recovery: Business Continuity through Data Archival and Retrieval Systems

The ability to maintain business continuity begins with proper backup systems. Backup hardware and software is the foundation of our Disaster Recovery/Business Continuity Plan, with all local business data backed up daily, weekly, monthly and yearly. A contracted data storage vendor rotates these backups to an off-site storage facility.

Besides ensuring that data is backed up properly, we have taken many additional steps to ensure business continuity if a major event takes place at the Primary Data Center in Phoenix. This includes additional server-class machines placed in an alternate location as warm stand-bys. From this location, the ValueOptions Information Services staff has the capability of restoring the data retrieved from our offsite storage vendor with a backup SDLT tape drive and resume business operations. ValueOptions also currently uses DFS (Distributed File System) to replicate specific data to alternate server locations in "real time". In addition, ValueOptions utilizes a redundant reporting server, which can be run in parallel to our primary reporting server for testing purposes or for disaster recovery.

An offsite warehouse with business recovery supplies is also maintained with more than 150 computer systems, backup printers, fax machines, and a spare phone system. Additionally, there are over 300 users with laptops that can all access our main business systems and data remotely. Access is available via direct dialup or VPN connection both locally in Phoenix and through ValueOptions' Corporate offices in Reston Virginia.

With regard to telecommunication systems and crisis lines, all Direct Service Sites have the capability to be backup sites should access to the main administrative offices be disrupted. These locations have upgraded phone systems that can handle our crisis call center traffic in addition to regular business calls. Additionally, we have an out of state "warm site" that calls can be routed to as another level of security.

While current systems and plans provide a solid platform for Disaster Recovery and Business Continuity, ValueOptions understands that we must continually enhance our systems to keep up with current technology and defend against new threats. With this goal in mind, the next section outlines ValueOptions' plan for the future.

Disaster Recovery/Business Continuity Upgrade Project (See figure 5h-B for visual project details)

The following information outlines the Disaster Recovery/Business Continuity Upgrade Project scheduled for completion by mid 2004. This upgrade project is designed to provide complete network and major business system access redundancy for the State of Arizona as well as for ValueOptions Providers, Direct Service Sites, and employees if a major event were to occur at the primary Administrative facility in Phoenix.

Under this design, a second “mirror” site will be installed in a designated existing ValueOptions Direct Service Sites (Secondary Site). This location will be on a separate power grid and central office away from the primary hub location at the Phoenix Administrative offices (Primary Site). The facility will have its own fire suppression, power backup, temperature control and security systems, and will provide complete redundancy for all local primary business systems and for connectivity to ValueOptions Corporate business systems in Virginia.

Wide Area Network (WAN) traffic for half of the local Direct Service Sites will be rerouted to this secondary site for load balancing. Each Direct Care Site will have a primary T1 connection to one of these two sites with a secondary failover T1 connection to the other. Each Direct Care Site will have tertiary connectivity via either a Cox Cable connection (where available) or a Qwest DSL circuit, which will provide VPN connectivity directly to the ValueOptions Corporate Offices in Virginia as well as the Arizona Primary site.

In addition to the WAN connectivity added by this mirror site, backup operations servers will also be located in this Secondary site. The HP NetServer (VO-PHX-DWH1) will be relocated to this location and will be upgraded and reconfigured to mirror the current active Data Warehouse (VO-PHX-SQL01), thereby offering data redundancy. Finally, the backup SDLT tape system will be relocated to this location for system recovery from the backup library should the need arise.

This comprehensive structure provides a platform for complete redundancy of network connectivity, as well as for all major business systems located in the Arizona ValueOptions Service Center. In the event of a disaster at either the primary or secondary site, business operations would be able to continue with almost full functionality within a matter of a few hours. In the event a major disaster should take down both central locations, Direct Service Sites would still have independent connectivity to the major ValueOptions business systems via their VPN connections to the corporate offices.

As well as systems internal to ValueOptions, this project will also include a Phase One assessment and analysis of the current Disaster Recovery/Business Continuity Plans for all connected providers to assist them in their endeavor to ensure the availability of systems and data should an adverse situation arise.

The utilization of multiple geographic locations, data paths, servers, utilities, and providers allows for flexibility and resiliency in our network and business systems, offering the greatest chance of success for Business Continuity should a disaster strike. This further demonstrates ValueOptions’ commitment to ensuring the safety, integrity and availability of ValueOptions’ business systems and services to all of its customers.

Backup Hardware

The ValueOptions Arizona Service Center utilizes a PowerVault 128T SDLT (Tape Library) for all local system backups. This device is a high-speed, high capacity unit. It is capable of holding a maximum of 20 SDLT tapes, for a total of approximately 4.4 TeraBytes of backup capacity. The PowerVault 128T is equipped with an optical scanner to automate the inventory of backup tapes, and a management password is required to prevent unauthorized removal of tape media from the library. The PowerVault 128T has been sectioned into two partitions. Partition one consists of tapes 1 through 15 and partition two contains tapes 16 through 20. Creating partitions helps remove the chance of unwanted overwrites of media and allows for monthly backups without skipping a weekly rotation. This backup hardware is protected by a 24 hour per day, 7 day per week, 365 day per year warranty on all hardware with a 4-hour on-site response time as needed. In addition, ValueOptions utilizes a Quantum SDLT 110/220 drive, stored at an off-site location, as an emergency backup solution for immediate restores should the PowerVault library become unavailable.

Backup Software

The backup server operating system platform is Windows 2000 Server running Service Pack 4. The media backup software is Backup Exec Version 8.6 Rev. 3878, licensed for library expansion, open file, Remote Agent, SQL Server and Exchange Server. By using Backup Exec software, ValueOptions is able to utilize the PowerVault 128T partitions; setting weekly backups on the first partition, tapes 1 through 15, and monthly and annually on the second partition, tapes 16 through 20. This method of data backup allows the data to be written to only specific partitions. Backup Exec also utilizes the optical barcode scanner capability of the PowerVault 128T to inventory what specific data is being stored on each tape as it runs. The tape ID is received from the optical scanner and the information is stored in the Backup Exec database.

Tape Storage/Rotation

As previously mentioned, backup tapes stored in the PowerVault 128T cannot be removed without an administrator password that only the LAN employees possess. All tapes are inventoried weekly to confirm the location of archived data, and all tape rotations are logged using the unique barcode ID. Full backups are done daily and rotated weekly with an eight-week expiration. We store seven weeks of backup tapes on-site and one set of two-week-old tapes off-site, which are rotated on a weekly basis. In addition, monthly and annual backups are completed and all are stored off-site once completed. (See figure 5h.1 below)

For the safety and security of all ValueOptions backup data, a third party contract has been established with DataPro, a professional storage company, for the protected off-site storage of all ValueOptions Arizona Service Center backup tape libraries. DataPro has coordinated with ValueOptions to allow only designated staff to receive and deliver tapes to their couriers. All off-site backup tapes can be retrieved and delivered on-site within a 2-hour contracted window.

Figure 5h.1 Tape Storage/Rotation Schedule

Week	Weekly Set Created	Weekly Moved off-site	Weekly Returned	
Week 1	Week 1 Backup created			
Week 2	Week 2 Backup created			
Week 3	Week 3 Backup created	Week 1 Backup - off-site		
Week 4	Week 4 Backup created	Week 2 Backup - off-site	Week 1 Set Returned	
Week 5	Week 5 Backup created	Week 3 Backup - off-site	Week 2 Set Returned	
Week 6	Week 6 Backup created	Week 4 Backup - off-site	Week 3 Set Returned	
Week 7	Week 7 Backup created	Week 5 Backup - off-site	Week 4 Set Returned	
Week 8	Week 8 Backup created	Week 6 Backup - off-site	Week 5 Set Returned	

Week	Monthly Set Created	Monthly Stored off site	Yearly Set Created	Yearly Moved off-site
Week 1				
Week 2				
Week 3				
Week 4	Month 1 Backup created			
Week 5		Month 1 Backup - off-site		
Week 6				
Week 7				
Week 8	Month 2 Backup created			
Week 9		Month 2 Backup - off-site		
Week 52			Yearly Set created	
Week 1				Yearly 1 Backup - off-site

Telephone Backup Systems

- The Meridian 1 phone system, Custom Call Routing (CCR) system, and Meridian Max are backed up to tape daily.
- Meridian Mail system programming is backed up to tape weekly and is rotated monthly.
- The Voice Recorder System Data is backed up daily by a MO (Magnetic Optical) disc drive and is stored for five years.

- The Database Manager system data is backed up by a DDS3 tape drive daily. Tape sets are rotated weekly.

ValueOptions Corporate Offices-Virginia

Backup Hardware/Software

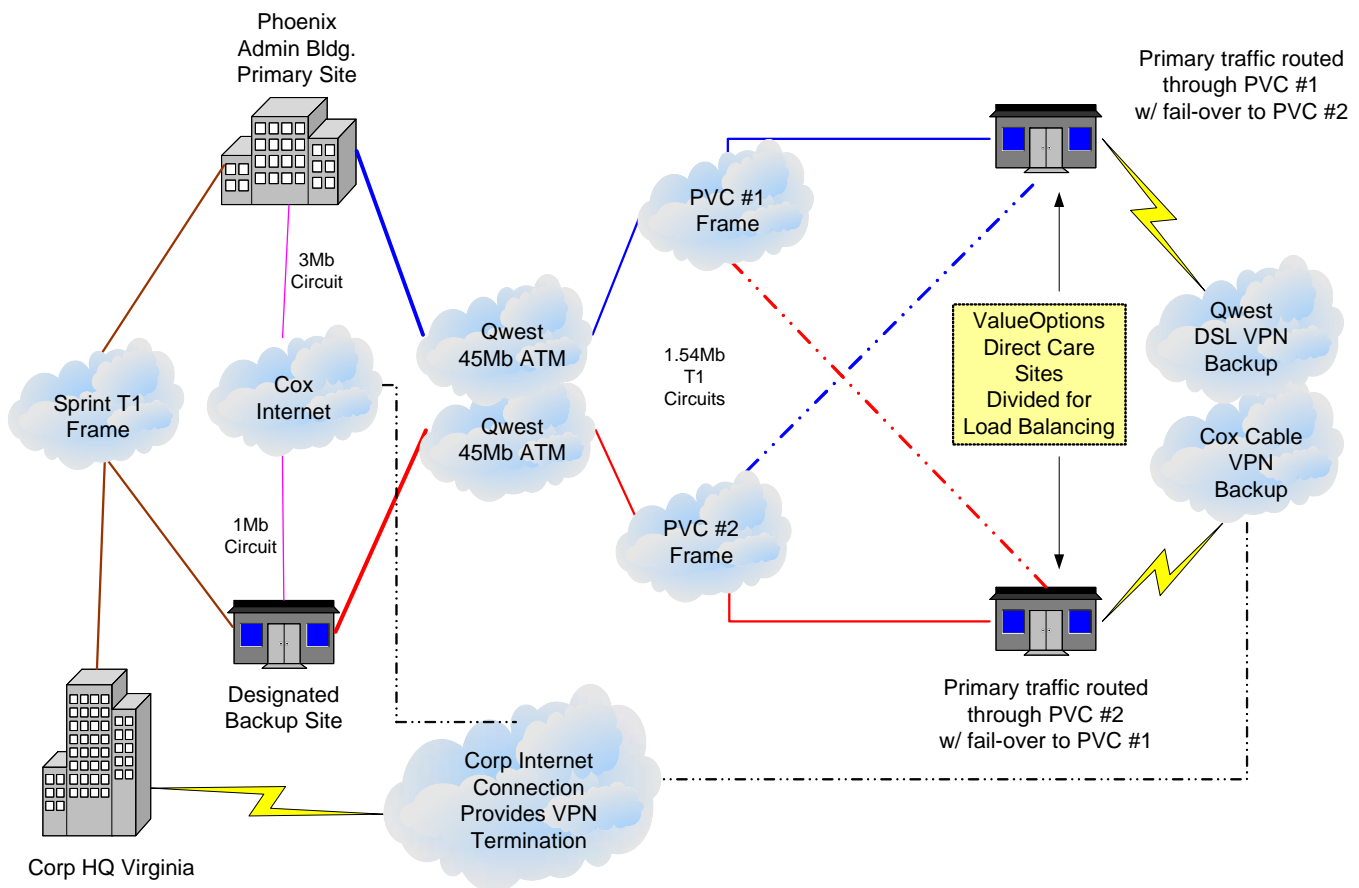
- Save and restore operations for our IBM AS/400 and iSeries platform environments are executed through the use of IBM's Backup, Recovery and Media Systems (BRMS) licensed software.
- Save and restore operations for our Unix and Intel-based operating system environments are executed through the use of IBM's Tivoli Storage Manager (TSM) licensed software.
- Both TSM and BRMS share a partitioned IBM 3494 Automated Tape Library to carry out automated tape read/write operations through LAN and serial based communication with TSM and BRMS host servers. The utilization of BRMS and TSM in conjunction with an automated tape library allows us to store critical data onsite while maintaining a duplicate copy of all data offsite at a certified data storage facility.

Rotation

Backup data retentions are determined by the nature of the information collected and by future retrieval requirements. All ValueOptions claims and financial data are retained for seven years, and MHS and Finance/HR data are backed up daily.

- Daily backups consist of a cumulative save-change-object (more commonly referred to as an "incremental") of application data and is retained for 90 days.
- Weekly backups consist of a full database save of all application and system data, which is retained for 90 days.
- Monthly backups consist of a full database save of all application and system data, which is retained for 13 months.
- Annual backups consist of a full database save of all application and system data, which is retained for seven years.

Figure 5h.2 Back-up Connectivity



i. System Security and Audit Trail

In today's volatile business environment, security is of the utmost importance. Steps must be taken on an on-going basis to maintain the confidentiality, integrity and availability of company and consumer information. New threats that could jeopardize this highly confidential information arise from different channels almost daily. In addition, legislation such as the Health Information Portability and Accountability Act (HIPAA) adds additional requirements regarding how this information must be protected.

ValueOptions has put in place numerous security measures to protect the confidential information we deal with on a daily basis—from a full Demilitarized Zone (DMZ) with multiple layers of firewalls to keep outsiders out, to extensive access control security to ensure that privileged information is accessible only to those who need it.

Regular surveys and audits are completed throughout all areas to ensure operational compliance with regulations and security measures. These security measures are monitored and constantly evaluated against industry standards and known threats, to ensure that the ValueOptions systems and networks can provide the utmost safety and security for all ValueOptions, State, provider, and consumer information. Below is a summary of these measures. The first section deals with ValueOptions server and system security; the second section provides information on the ValueOptions network.

System/Server Security

System data are protected at multiple layers and with multiple systems—primarily at the operating system level by NT security, and at the application level utilizing SQL and Sybase assigned rights.

NT Security

To gain access to any application that contains ValueOptions data, one must be able to logon to the ValueOptions network. Network logons are controlled and assigned to employees and contractors based on their job functions or role with the company. The appropriate security access forms are submitted to a manager for approval, and are reviewed by the Information Services manager before submission to ValueOptions corporate office for review. Only selected Information Services administrative staff is granted local access to the data warehouse servers.

Each workstation on the ValueOptions network is secured by the same access requirements mentioned above. In addition, only ValueOptions Information Services technical and administrative employees have rights to install, upgrade or make programming changes to any workstations. Each workstation is configured with security screensavers that lock the workstation after 5 minutes of inactivity, requiring the user or an administrator to unlock it. The ValueOptions Information Services employees handle all upgrades, patches, or policy changes to workstations.

SQL and Sybase Login Security

Only the Data Warehouse Manager and the Database Administrator are able to grant access to the SQL and Sybase servers. Once access is granted, it is then tied to the user's NT account so that any action that is taken is logged to that specific user. Even users with access do not have direct access to the raw data tables; instead, they are granted access to a separate workspace on the network where they can create the reports and access the data they need, without having the ability to alter original data.

Anti-Virus Software – Norton Anti-Virus Corporate Edition

Servers are scanned daily for viruses, and live automatic virus software and definition update scans are performed daily as well. If viruses are found, Norton Antivirus software quarantines and cleans the virus from the system automatically. In addition, Norton Antivirus Console is utilized by PC technicians and administrative staff to screen user PC's and servers throughout the entire network for viruses. Policies governing incident handling, and system compromise situations, have been put in place and are all part of the comprehensive security policies currently in place.

Login Security Auditing

Security auditing is enabled on servers to generate Security Log Files, which track successful and unsuccessful network and server resource access attempts. These logs are filtered and reviewed frequently by administrative IT staff.

Network Security (See figure 5i.1 for visual details)

ValueOptions uses a "Layered Security Model" approach to protect its network infrastructure and the connected systems. There are several aspects to this approach, which are each addressed below.

Firewalls

ValueOptions utilizes Nokia Checkpoint Firewalls at the outer perimeter of its network to protect the internal network from unwanted externally initiated connections. The firewall uses Network Address Translation (NAT) to mask the internal IP addresses bound for the Internet into one “shared” external IP address. Providers that have a frame-relay connection to ValueOptions must pass through this firewall, which is configured to allow access based on source and destination address, as well as on destination ports. The Demilitarized Zone (DMZ) is configured to allow typical Web traffic while all other ports are blocked. The switch is monitored with an Intrusion Detection System (IDS). Tests are run from the outside monthly or as needed to ensure that there are no vulnerabilities in the Web server or the firewall.

Access Control Lists/Null Routing

All network routers utilize Standard and Extended Access Control Lists (ACL) to filter and pass permitted network traffic and to block all other traffic. In addition to filtering, questionable traffic is routed to a null interface, causing the traffic to be dropped.

Logging

Syslog is configured on two Linux Servers, (Syslog 1 & 2) running Linux RedHat 9.0. All access to network devices (Routers/Switches) is logged. Any traffic that is denied access to the network is logged. The Syslog servers are configured to e-mail LAN administrators once an hour with all logging that took place the previous hour. Urgent logs are tagged and e-mailed immediately. The Linux Servers have Port-Sentry configured and notify the Administrators if any port-scans have been run on the network.

TACACS+ (Terminal Access Controller Access Control System)

TACACS+ is a server-based application that handles accounting, authentication, and authorization for all network routers and switches. All access to the routers and switches are controlled through the TACACS+ servers, which hold the assigned administrative usernames and passwords. TACACS+ runs on two Linux Servers (Syslog 1 & 2) running RedHat 9.0. The connection between the TACACS+ servers and the routers/switches require a matching key to be configured on both ends for a successful connection. The passwords are encrypted at 168bits on the TACACS+ server and expire every 90 days. All access, including any configuration changes to the routers and switches, is logged.

Intrusion Detection Systems

Two Intrusion Detection Systems (IDS) are deployed on the network. One IDS server monitors all traffic to and from our network internally, and the other IDS server monitors all traffic on the DMZ switch. Both IDS systems are on Linux Servers running RedHat 9.0 using Snort, an open source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. Snort can perform protocol analysis and content searching/matching and can be used to detect a variety of attacks and probes.

All Linux Servers are configured to disallow access to critical core operating system files. Acid is the application used to view IDS data across a Secure Sockets Layer (SSL) connection, a connection that provides the highest level of online security. IDS data is logged and certain events that are marked “urgent” are e-mailed to the administrators. IDS rules/signatures are updated as updates become available.

The primary function of these systems is to monitor attempts to breach security from inside of the ValueOptions network by unauthorized users trying to gain access to secured network areas or functions, as well as to protect information from outside intruders attempting to gain unauthorized access into the network. In addition, “honeypots”, decoy servers or systems, have been deployed within the network to bait unauthorized users away from critical systems and give administrators the opportunity to monitor and track these unauthorized users until their source can be located and legal action taken.

Server Communication Security

All connections to the Linux Servers are done through SSH connections, a secure connection protocol. SFTP (Secure File Transport Protocol) is the only file transfer protocol that is allowed on the Linux servers. Web access to the Linux Servers is provided through highly secure SSL connections. SNMP (Simple Network Management Protocol) is used with unique community strings as well as ACLs to ensure layered security. User authentication, as well as ACLs, controls access to all routers. Where applicable, more secure SSH connections are used to connect to routers/switches instead of telnet. Passwords on

all routers/switches are encrypted, ensuring that even if such information were to end up in the wrong hands, it would be unreadable and thus unusable.

Virtual Private Network

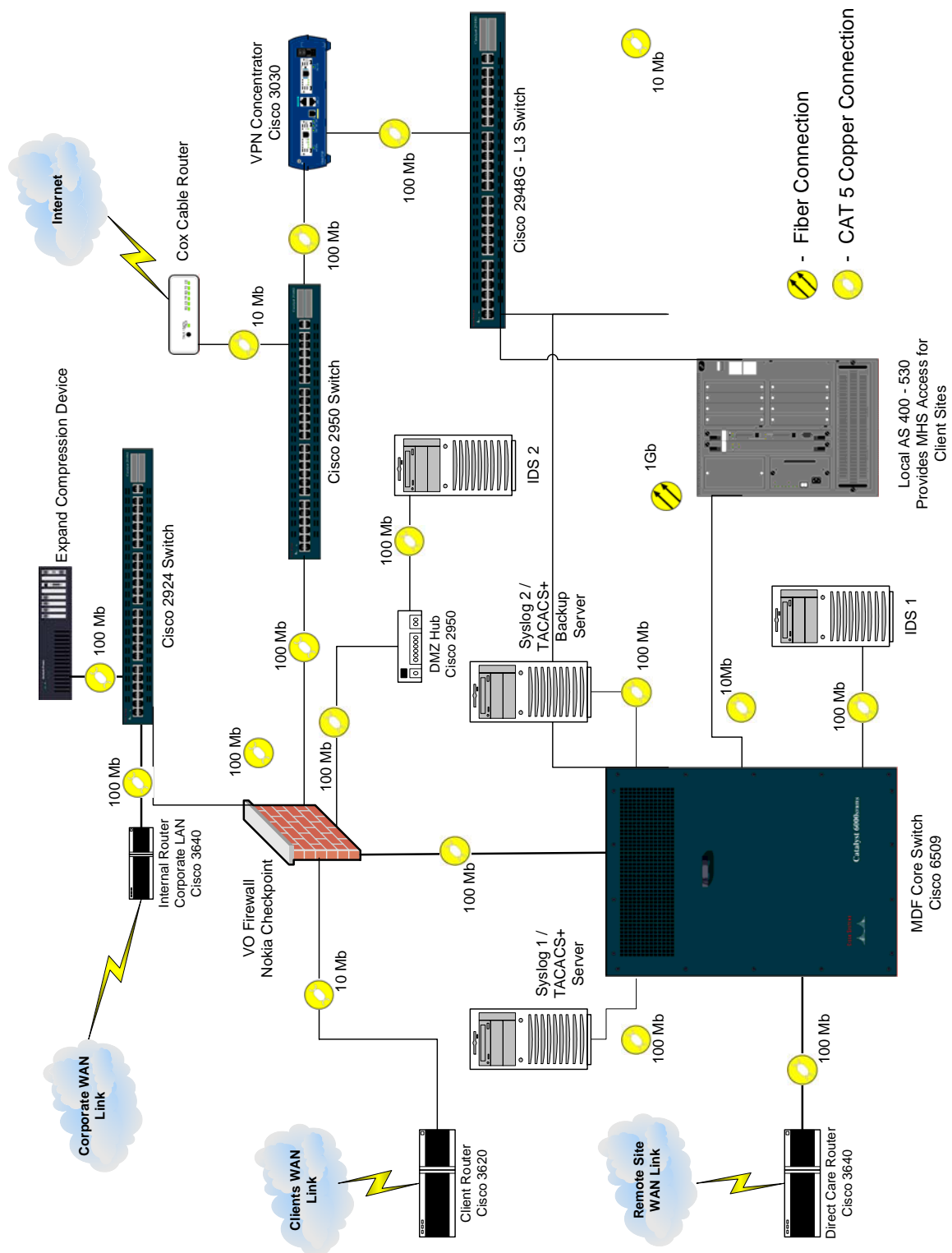
ValueOptions uses a Cisco 3030 Concentrator to terminate Virtual Private Network (VPN) sessions. This system creates a virtual private network by creating a secure connection across a TCP/IP network (such as the Internet) that users see as a private connection. Using a 168 bit encryption 3DES, the Concentrator ties into our Windows Network for user authentication. It is a requirement that the end user be connected through a remote firewall (software/hardware) when connecting into our system through VPN.

In addition, the ValueOptions Arizona Service Center also uses VPN as a redundant connection to our Virginia Corporate office in situations where the Frame-Relay circuit is down. The connection is passed through a Cisco 3640 router on each end that provides 3DES/Ipsec/FW security for the connection.

Vulnerabilities/Virus Notifications

ValueOptions administrative employees belong to several e-mail lists and forums that send notification when new vulnerabilities have been discovered. Notices are also sent to management regarding virus updates or new service packs or system "patches". Having this information provides us with a proactive approach to patching or upgrading software and allows us to implement temporary routers or firewall configuration changes before being adversely affected. All upgrades, service packs, and/or patches are applied and tested on non-critical, non-production systems first to ensure compatibility with existing configurations before release into the production environment.

Figure 5i.1 Arizona ValueOptions Firewall / IDS Configuration



j. Information Systems Data Mapping

By ensuring the timely receipt of data, the ValueOptions' Information Services Department helps the behavioral health system in Maricopa County to operate more efficiently and effectively. In addition, our ability to store large amounts of data, and to organize this data in a way that is easily utilized, provides us a way to create demographic summaries and to analyze data such as penetration rates. This ability to efficiently transfer and store data benefits the behavioral health system by saving resources, time and money and by allowing these resources to be relocated to provide better services to our consumers.

Currently, ValueOptions has systems in place to store data as required by the Client Information System (CIS) File Layout and Specifications Manual. Below is a complete mapping of required data, listed by its current format in our system. This description documents the mapping of data elements collected by ValueOptions Managed Healthcare System (MHS) and passed to CIS.

These data elements are submitted to ADHS/DBHS and represent the minimum data necessary for ADHS/DBHS and ValueOptions to conduct their oversight and regulatory functions. For transaction purposes, all data transmitted to the State by ValueOptions maintains the same format as the data received from providers. As you will see from the charts and data mapping that follow, all required HIPAA and CIS File Layout requirements are currently in-place and are being exchanged as specified in the contract.

Transaction Tables

Table/Extract: Demographic

Description:

All consumers who receive service through the RBHA system must have current demographic data in CIS. Demographic information is time-sensitive and intended to reflect changes in consumers' demographic, financial, clinical, and categorical eligibility status. All consumers who remain enrolled for more than 30 days must have Demographic Data submitted within 45 days of enrollment. Unless otherwise noted, all items must be completed for Demographic Data submissions. Demographic Data are submitted at enrollment, when data information changes and annually thereafter; identified elements are submitted at disenrollment.

Purpose/Uses

The Demographics file is a required file by the Department of Behavioral Health Services. This file is submitted to DBHS when new consumers are enrolled into CIS. This file is a collection of required demographics and clinical information.

Column Definitions

CIS	Client Information System field
MHS	Mental Health System (MHS) field
Data Type	Type of data stored in field
Length	Length of field
Description/Exclusions	Description of data stored in field
Logic	Supporting logic

Demographic Data File Format –(T)RBHA Reporting Requirements

* Denotes data that is stored in a different format than is transmitted – see Description /Exclusion.

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
RBHA-ID	Defaulted	char	2	RBHA Identification Number. Valid values: 03 = Excel Group 08 = ValueOptions 11 = Gila River Indian Tribe 14 = Navajo Nation 15 = NARBHA	Always '08'

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
				23 = PGBHA 25 = Pascua Yaqui 26 = CPSA 5 27 = CPSA 3	
Reason-for-Submission	Defaulted	char	1	Indicates Transaction Type: 1 = Initial Intake 2 = Complete Update 3 = Change 4 = Disenrollment	
Client-ID	membno	char	10	The unique CIS identifier for the client.	
Intake-Date	enrdat	date	8	Initial intake date.	
Client-First-Name	fstnam	char	25	Client's first name.	
Client-Middle-Name	midnam	char	25	Client's middle name.	
Client-Last-Name	lstnam	char	35	Client's last name.	
Date-of-Birth	bthdat	date	8	Client's date of birth.	
Referral-Date	refdat	char	8	This is the date that the client first requested an appointment.	
Referral-Source	rrsrc	char	2	The Source of client referral Valid Values: 01 – Self/family/friend 03 – Other behavioral health provider 19 – Other (VA, HIS, etc) 35 – AHCCCS health plan 36 – CPS 37 – Other community agency (homeless shelter, church, employer) 38 – Other state agency – child serving 39– Other state agency – adult serving 40–Criminal justice/ correctional	
OMB – American Indian *	racecd-must convert	char	1	OMB Race Category – Is client American Indian or Alaska Native? Valid Values: Y for Yes, N for No (Default)	If racecd = '05' then 'Y'
OMB – Asian *	racecd-must convert	char	1	OMB Race Category – Is client Asian? Valid Values: Y for Yes, N for No (Default)	If racecd = '04' then 'Y'
OMB – Black *	racecd-must convert	char	1	OMB Race Category – Is client Black or African American? Valid Values: Y for Yes, N for No (Default)	If racecd = '02' then 'Y'
OMB – Native Hawaiian *	racecd-must convert	char	1	OMB Race Category – Is client Native Hawaiian or Pacific Islander? Valid Values: Y for Yes, N for No (Default)	If racecd = '08' then 'Y'
OMB – White*	racecd-must convert	char	1	OMB Race Category – Is client White? Valid Values: Y for Yes, N for No (Default)	If racecd = '01' then 'Y'
OMB – Hispanic-Latino *	racecd-must convert	char	1	OMB Race Category – Is client Hispanic or Latino? Valid Values: Y for Yes, N for No (Default)	If racecd = '03' then 'Y'
PC-Suicidal *	priprb code must be converted	char	1	Presenting Concern – Suicidal/DTS Valid Values: Y for Yes, N for No (Default)	If = '01' then 'Y' else default to 'N'
PC-Assaultive	priprb code	char	1	Presenting Concern – Assaultive/DTO	If = '18' then

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
*	must be converted			Valid Values: Y for Yes, N for No (Default)	'Y' Else Default to 'N'
PC-Victim-ANV *	priprb code must be converted	char	1	Presenting Concern – Victim of Abuse/Neglect/Violence Valid Values: Y for Yes, N for No (Default)	If = '02' then 'Y' Else Default to 'N'
PC-Anxiety-Stress *	priprb code must be converted	char	1	Presenting Concern – Anxiety/Stress Valid Values: Y for Yes, N for No (Default)	If = '03' then 'Y' Else Default to 'N'
PC-Depressed *	priprb code must be converted	char	1	Presenting Concern – Depressed Mood Valid Values: Y for Yes, N for No (Default)	If = '04' then 'Y' Else Default to 'N'
PC-Psychotic *	priprb code must be converted	char	1	Presenting Concern – Psychotic (impaired reality, thought disorganization) Valid Values: Y for Yes, N for No (Default)	If = '05' then 'Y' Else Default to 'N'
PC-Unable-to-Care *	priprb code must be converted	char	1	Presenting Concern – Unable to care for self (dehydrated, malnourished, malodorous) Valid Values: Y for Yes, N for No (Default)	If = '13' then 'Y' Else Default to 'N'
PC-Relational*	priprb code must be converted	char	1	Presenting Concern – Family relational problem Valid Values: Y for Yes, N for No (Default)	If = '10' then 'Y' Else Default to 'N'
PC-Child-Behavior *	priprb code must be converted	char	1	Presenting Concern – Child behavioral problem Valid Values: Y for Yes, N for No (Default)	If = '16' then 'Y' Else Default to 'N'
PC-Other *	priprb code must be converted	char	1	Presenting Concern – Other Valid Values: Y for Yes, N for No (Default)	If = '14' then 'Y' Else Default to 'N'
Descr-Char-Eff-Date *	To be added to MHS - but captured in Data Warehouse	date	8	Effective date of descriptive characteristics addition or change.	
Household-Size	hsize	char	2	Number in household including client. Valid numbers 01-99.	
Household-Income	hincom	char	6	Gross Annual Income of household of the client	
Treatment-Participation	nattrt	char	1	Treatment participation reason under which a client enters the facility or service. Valid Values: 1 = Voluntary 6 = Civil or MH Court Order 7 = DUI Court Order 8 = Criminal Court Order	
OA-ADC-	agdc	char	1	Other Agency – ADC-Parole	

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
Parole				Valid Values: Y for Yes, N for No (Default)	
OA-ADJC-Parole	agadjc	char	1	Other Agency – ADJC-Parole Valid Values: Y for Yes, N for No (Default)	
OA-ADHS-CRS		char	1	Other Agency – ADHS/CRS Valid Values: Y for Yes, N for No (Default)	
OA-AOC-Adult-Probation	agcap	char	1	Other Agency – AOC-Adult-Probation - Valid Valid Values: Y for Yes, N for No (Default)	
OA-AOC-Juvenile-Probation	agcjp	char	1	Other Agency – AOC-Juvenile-Probation Valid Values: Y for Yes, N for No (Default)	
OA-DES-CPS	To be added to MHS - but captured in Data Warehouse	char	1	Other Agency – DES-CPS Valid Values: Y for Yes, N for No (Default)	
OA-DES-DDD	agddd	char	1	Other Agency – DES-DDD Valid Values: Y for Yes, N for No (Default)	
OA-DES-RSA	To be added to MHS - but captured in Data Warehouse	char	1	Other Agency – DES-RSA Valid Values: Y for Yes, N for No (Default)	
OA-DES-Jobs	To be added to MHS - but captured in Data Warehouse	char	1	Other Agency – DES-Jobs Valid Values: Y for Yes, N for No (Default)	
OA-School-Special-Ed	To be added to MHS - but captured in Data Warehouse	char	1	Other Agency – School-Special-Ed Valid Values: Y for Yes, N for No (Default)	
OA-Other	To be added to MHS - but captured in Data Warehouse	char	1	Other Agency – Other Valid Values: Y for Yes, N for No (Default)	
Formal-Schooling-Level	schyrs	char	1	Highest Formal School Level Completed Valid Values: 1 = Less than 1 year. 2 = Grades 1 to 11 3 = High School Graduate or GED 4 = Vocational/ Technical School 5 = Some college, no degree 6 = AA/BA degree 7 = Graduate or Post-graduate 8 = Unknown	
SF-COOL	spopcd (ref code = '05')	char	1	Indicates source of special funding from COOL. Valid Values: Y for Yes, N for No (Default)	
SF-HB2003	spopcd (ref code = '07' or	char	1	Indicates source of special funding from HB2003.	

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
	'08')			Valid Values: Y for Yes, N for No (Default)	
SP-Pregnancy	sppreg	char	1	Indicates that the client is a pregnant or post-partum woman. Valid Values: Y for Yes, N for No (Default)	
SP-Woman-DC	spwdch	char	1	Indicates that the client is a woman with dependent children. Valid Values: Y for Yes, N for No (Default)	
AXIS-III-1	To be added to MHS - but captured in Data Warehouse	char	2	Axis III Medical Condition. Valid Values: 00 = N/A 01 = Infectious and parasitic diseases. 02 = Neoplasms 03=Endocrine, nutritional, metabolic diseases, and immunity disorders. 04 = Diseases of the blood and blood-forming organs. 05 = Diseases of the nervous system and sensory organs. 06 = Diseases of the circulatory system. 07 = Diseases of the respiratory system. 08 = Diseases of the digestive system. 09 = Diseases of the genitourinary system. 10 = Complications of pregnancy, childbirth, puerperium. 11 = Diseases of the skin and subcutaneous tissues. 12 = Diseases of the musculoskeletal system and connective tissues. 13 = Congenital anomalies. 14 = Conditions originating in the prenatal period. 15 = Symptoms, signs, and ill-defined conditions. 16 = Injury or poisoning.	
AXIS-III-2	To be added to MHS - but captured in Data Warehouse	char	2	Axis III Medical Condition. Valid Values: Same as with AXIS-III-1.	
AXIS-III-3	To be added to MHS - but captured in Data Warehouse	char	2	Axis III Medical Condition. Valid Values: Same as with AXIS-III-1.	
AXIS-III-4	To be added to MHS - but captured in Data Warehouse	char	2	Axis III Medical Condition. Valid Values: Same as with AXIS-III-1.	
AXIS-III-5	Not collected to be added to MHS - but	char	2	Axis III Medical Condition. Valid Values: Same as with AXIS-III-1.	

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
	captured in Data Warehouse				
Outcome-Measures-Eff-Date	Not collected to be added to MHS - but captured in Data Warehouse	date	8	Effective date of outcome measures addition or change.	
AXIS-I-1	dsma1p	char	6	ICD-9 Axis I Primary Medical Condition. Denotes clinical syndromes. Valid ICD-9 Code – 6-byte format is XXX.XX	
AXIS-I-2	dsma1a	char	6	ICD-9 Axis I Secondary Medical Condition. Denotes clinical syndromes. Valid ICD-9 Code – 6-byte format is XXX.XX	
AXIS-I-3	Not collected to be added to MHS - but captured in Data Warehouse	char	6	ICD-9 Axis I Tertiary Medical Condition. Denotes clinical syndromes. Valid ICD-9 Code – 6-byte format is XXX.XX	
AXIS-I-4	Not collected to be added to MHS - but captured in Data Warehouse	char	6	ICD-9 Axis I Additional Medical Condition. Denotes clinical syndromes. Valid ICD-9 Code – 6-byte format is XXX.XX	
AXIS-I-5	Not collected to be added to MHS - but captured in Data Warehouse	char	6	ICD-9 Axis I Additional Medical Condition. Denotes clinical syndromes. Valid ICD-9 Code – 6-byte format is XXX.XX	
AXIS-II-1	dsma2p	char	6	ICD-9 Axis II Primary Medical Condition. Denotes developmental and personality disorders. Valid ICD-9 Code – 6-byte format is XXX.XX	
AXIS-II-2	dsma2a	char	6	ICD-9 Axis II Secondary Medical Condition. Denotes developmental and personality disorders. Valid ICD-9 Code – 6-byte format is XXX.XX	
Behavior-Health-Category *	rbhafs	char	1	Behavioral health category. Valid values: C = Child Z = Child, with SED S = Adult, with SMI M = Adult, non-SMI, with general mental health need G = Substance abuse	If this field = 'c' then 'c', else if field = 'c' and SMI/SED field = 'y' then = 'z', else if field = 's' then 's', else if field = 'm' then 'm', else if field = 'd' or 'a' then 'g'

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
Employment-Status	empsta	char	2	Employment-status. Valid Values: 01 = Employed full-time without support 02 = Employed part-time without support 03 = Employed full-time with support 04 = Employed part-time with support 08 = Unemployed 14 = Volunteer 17 = Unpaid rehabilitation activities 18 = Retired, homemaker, or student 99 = Unknown	
Educational-Status *	edstat	char	1	Educational status. The client is in a school or vocational program. Valid Values: Y for Yes, N for No (Default)	if '01' or '02' then = 'y' else 'n'
Primary-Residence	prires	char	2	Primary place of residence. Valid Values: 01=Independent (roommate, by self, no support) 02 = Hotel 03 = Boarding home 04 = Supervisory care/assisted living 05 = Arizona State Hospital 06 = Jail/prison/detention 07 = Homeless/homeless shelter 08 = Other 09 = Foster home 12 = Nursing home 16 = Home with family 19 = Crisis shelter 22 = OBHL Level 1, 2, or 3 treatment setting 23 = Transitional housing (level 4)	
AXIS-V	Not collected to be added to MHS - but captured in Data Warehouse	char	3	Axis V Global Assessment Functioning. Two-digit CGAS/GAF score. Valid Values: 01 – 100. See Demographic Definitions for detail.	
Number-of-Arrests	arrest	char	2	For initial intake, number in 6 months prior to intake and for updates/disenrollment, the number since last data update. Valid values are 00-99.	
SA-Type-1	sbtyp1	char	4	Current Substance Abuse Primary type Valid Values: 0001 – None Depressants: 0201 – Alcohol 1308 – Other Benzodiazepines Stimulants 1605 – Other Sedatives 0302 – Cocaine/Crack 1703 – Other Inhalants 1001 – Methamphetamine/Speed 2002 – Other Drugs 1201– Other Stimulants 0401–Marijuana/ Hashish	

CIS	MHS	Data Type	Length	Description/ Exclusions	Logic/ Comment
				Opiates/Narcotics: 0501 – Heroin/Morphine 0706 – Other Opiates/ Synthetics 0902–Other Hallucinogens	
SA-Freq-1	sbfrq1	char	1	Freq-sub-use, Type: Primary Valid Frequency Values: 1 = No use past month 2 = 1-3 times in past month 3 = 1-2 times per week 4 = 3-6 times per week 5 = One or more times per day	
SA-Route-1	sbrte1	char	1	Route of administration Primary Valid Route Values: 1 = Oral 2 = Smoking 3 = Inhalation 4 = Injection 5 = Other	
SA-Age-First-Use-1	sbage1	char	2	Age of first use of SA-Type-1	
SA-Type-2	sbtype2	char	4	Current Substance Abuse Secondary Type Select a valid code from above list, but must not be the same as the one used for SA-Type-1.	
SA-Freq-2	sbfrq2	char	1	Freq-sub-use, Type: Secondary. Use same values as in SA-Freq-1.	
SA-Route-2	sbrte2	char	1	Route of administration Secondary. Use same values as in SA-Route-1.	
SA-Age-First-Use-2	sbage2	char	2	Age of first use of SA-Type-2	
Past-SA-Type		char	4	Past Substance Abuse. Select a valid code from list at SA-TYPE-1.	
Reason-for-Disenrollment	disrsn	char	2	Indicates the reason for the disenrollment. Valid values: 01=Treatment completed 02=Change in Eligibility/Entitlement Information. 03=Client Declined Further Service 04=Lack of contact 06=Incarceration 07=Death 08=Moved out of area 09=Inter RBHA Transfer 11= Other (If not being disenrolled, use default of spaces.)	

Table/Extract: 834 Intake – Add and Changes

Description

This is a HIPAA compliant file that is sent to CIS on a daily basis. The file contains current data for identifying consumers receiving services through ValueOptions. The data also contains closure and some demographic information that is collected in MHS from ValueOptions providers and Direct Service Sites.

Purpose/Uses

All consumers who receive service through the RBHA system must have current identifying data in the ADHS/DBHS CIS system. Intake information is time-sensitive and is intended to reflect current data for consumer identification and other consumer status items. All consumers who remain enrolled for more than 30 days must have Demographic Data submitted within 45 days of the initial enrollment.

CIS	MHS	Data Type	Length	Description
RBHA_ID		char	2	RBHA Name (Used to look up RBHA Number)
Action_Code		char	1	021=add(A)
rbha_client_id	tempno	char	10	RBHA Client_id
ahcccs_id	accsid	char	9	AHCCCS ID
client_id	membno	char	10	CIS Client ID
Intake_date / Closure_Date	enrdat	num	8	Intake Date (CCYYMMDD)
Last_Name	lstnam	char	15	Subscriber Last Name
First_Name	fstnam	char	10	Subscriber First Name
Middle_Int	midnam	char	1	Subscriber Middle Name
ssno	socsec	char	10	SSN
Address_Line_1	adrln1	char	25	Address Line 1
Address_Line_2	adrln2	char	25	Address Line 2
City	citycd	char	20	City
State	stacod	char	2	State
ZIP_Code	zipcod	char	9	ZIP
County_Residence	county	char	2	County (Location Identification code)
dob	bthdat	char	8	Date of Birth (CCYYMMDD)
sex	sexcod	char	1	Sex
Marital_status	marsta	char	1	Marital Status
Client_ethnicity	ethcod	char	2	Race/Ethnicity Code
Action_Code		char	1	021=add(A) 030=override (O)
intake_date	enrdat	num	8	Intake Date
Med_Insurance_1	medin1	char	1	Use names from table
Med_Insurance_2	medin2	char	1	Use names from table
Med_Insurance_3	medin3	char	1	Use names from table
Transfer_Record_count		num	8	Transaction segment Count

Table/Extract: 834 Closure– Add and Changes

Description

All consumers who receive service through the RBHA system must have current identifying data in the ADHS/DBHS Client Information System. Closure information is time-sensitive and is intended to reflect current identifying data and other consumer status items.

Purpose/Uses

The file is a HIPAA compliant file extract that is sent to Client Information System on a daily basis. This file is used to terminate consumers in MHS and CIS.

CIS	MHS	Data Type	Length	Description
-----	-----	-----------	--------	-------------

CIS	MHS	Data Type	Length	Description
RBHA-ID		char	2	RBHA Name (Used to look up RBHA Number)
Action_Code		char	1	001=change 024=termination
rbha_client_id	membno	char	10	RBHA Client_id
client_id	membno	char	10	CIS Client ID
Intake_date	enrdat	num	8	Intake Date (CCYYMMDD)
Closure_Date	enrdat	num	8	Closure Date (CCYYMMDD)
Last_Name	lstnam	char	15	Subscriber Last Name
First_Name	fstnam	char	10	Subscriber First Name
Middle_Int	midnam	char	1	Subscriber Middle Name
Ssno	socsec	char	10	SSN
Address_Line_1	adrln1	char	25	Address Line 1
Address_Line_1	adrln2	char	25	Address Line 2
City	citycod	char	20	City
State	statco	char	2	State
ZIP_Code	ZIPcod	char	9	ZIP
County_Residence	county	char	2	County (Location Identification code)
dob	bthdat	num	8	Date of Birth (CCYYMMDD)
sex	sexcod	char	1	Sex
Marital_status	marsta	char	1	Marital Status
Client_ethnicity	ethsta	char	2	Ethnicity

Table/Extract: 837I – Institutional Claims

Description

This file contains all the hospital claims that have been paid during the prior week. The file is sent to CIS weekly.

Purpose/Uses

This is a HIPAA compliant file that is used to send the UB92 (Inpatient hospital) claims to CIS for approval. After these claims are approved at BHS they are transmitted to AHCCCS for approval.

CIS	MHS	Data Type	Length	Description
Date	transfer-date	num	8	Transaction Set Creation Date
Time	transfer-time	num	8	Transaction Set Creation Time
Identification code	Rbha_id	char	2	RBHA Contractor Id
Reference Identification	Group-biller-id/Provider-id	char	9	Group Biller/Provider ID and Location
Reference Identification	Provider-id	char	9	Provider ID
Identification code	client-id	char	10	Client ID
Claim submitter's Identifier	ICN-Nbr	char	11	ICN Number
Facility Code Value	Bill-Type	char	2	Bill Type Position 1 and 2
Claim Frequency Type Code	Bill-Type/adjustment-flag	char	1	Bill Type Position 3
Date Time Period	Discharge-Hour	char	2	HHMM
Date Time Period	Service-Start-Date/End-Date	num	16	Statement Covers Period
Date Time Period	Admission-Dt & Admit-Hour	num	8	Date Time Period
Admission Type code	Admission-Type	char	1	Admission Type code

CIS	MHS	Data Type	Length	Description
Admission Source Code	Admission-Source	char	1	Admission Source Code
Patient Status Code	Patient-Status	char	2	Patient Status Code
Contract Type Code	svc-type	char	1	"05" or "02"
Monetary Amount	Special-Net-Value/Net-Paid	num	7	Special Net Value or Net-Paid
Reference Identification	Adjustment_icn	char	11	Claim Original Reference Number
Reference Identification	Prior-Auth-Nbr	char	6	Prior Authorization Number
Description	Dup-Override-Ind, Oth-Ins-Cov-Flag & Encounter-Processed-Date	char	10	String the three fields into a single 10 char entry
Industry Code	Diagnosis-code	char	6	Industry Code
Industry Code	Admit-Diag-cd	char	6	Industry Code
Industry Code	Trauma-code	char	6	Industry Code
Industry Code	Diagnosis-cd-1	char	6	Industry Code
Industry Code	Diagnosis-cd-2	char	6	Industry Code
Industry Code	Diagnosis-cd-3	char	6	Industry Code
Industry Code	Diagnosis-cd-4	char	6	Industry Code
Industry Code	Diagnosis-cd-5	char	6	Industry Code
Industry Code	Diagnosis-cd-6	char	6	Industry Code
Industry Code	Diagnosis-cd-7	char	6	Industry Code
Industry Code	Diagnosis-cd-8	char	6	Industry Code
Industry Code	ICD9-Proc-Code-1	char	4	Industry Code
Date time Period	ICD9-Proc-Date-1	char	4	Date time Period
Industry Code	ICD9-Proc-Code-2	char	4	Industry Code
Date time Period	ICD9-Proc-Date-2	char	4	Date time Period
Code List Qualifier Code				Code List Qualifier Code
Industry Code	ICD9-Proc-Code-3	char	4	Industry Code
Date time Period	ICD9-Proc-Date-3	char	4	Date time Period
Industry Code	ICD9-Proc-Code-4	char	4	Industry Code
Date time Period	ICD9-Proc-Date-4	char	4	Date time Period
Industry Code	ICD9-Proc-Code-5	char	4	Industry Code
Date time Period	ICD9-Proc-Date-5	char	4	Date time Period
Industry Code	Occurrence-Code-1	char	2	Industry Code
Date time Period	Occurrence-Date-1	num	8	Date time Period
Industry Code	Occurrence-	char	2	Industry Code

CIS	MHS	Data Type	Length	Description
	Code-2			
Date time Period	Occurrence-Date-2	num	8	Date time Period
Industry Code	Occurrence-Code-3	char	2	Industry Code
Date time Period	Occurrence-Date-3	num	8	Date time Period
Industry Code	Occurrence-Code-4	char	2	Industry Code
Date time Period	Occurrence-Date-4	num	8	Date time Period
Industry Code	Occurrence-Code-5	char	2	Industry Code
Date time Period	Occurrence-Date-5	num	8	Date time Period
Industry Code	Occurrence-Code-6	char	2	Industry Code
Date time Period	Occurrence-Date-6	num	8	Date time Period
Industry Code	Occurrence-Code-7	char	2	Industry Code
Date time Period	Occurrence-Date-7	num	8	Date time Period
Industry Code	Occurrence-Code-8	char	2	Industry Code
Date time Period	Occurrence-Date-8	num	8	Date time Period
Monetary Amount	Co-insurance	num	9	Monetary Amount
Reference Identification	Attending_Physician	char	9	Attending Physician
Monetary Amount	Oth-Ins-Pymt	num	8	Other Insurance Payment
Monetary Amount	Medicare-deductible	num	8	Medicare Deductible
Monetary Amount	Medicare-allow-amount	num	8	Medicare Allow Amount
Monetary Amount	Medicare-Payment	num	8	Medicare Payment
Assigned Number	Line_nbr	num	2	Line Number
Product/Service ID	Revenue-Cd	char	4	Service Line Revenue Code
Product/Service ID	Procedure_Code	char	5	Procedure Code
Monetary Amount	Billed_Amount	num	7	Line Item Charge Amount
Quantity	Unit-of-Service	num	7	Quantity
Monetary Amount	non-covered-chg	num	10	Line Item Non-Covered Charge Amt

Table/Extract: 837P Professional Claims

Description:

This file contains all the HCFA-1500 claims that have been paid in MHS. The file is sent to CIS daily.

Purpose/Uses:

This file is used to send the HCFA-1500 Claims to CIS for approval. These claims are approved at CIS monthly and are subsequently transmitted to AHCCCS for approval.

CIS	MHS	Data Type	Length	Description
Date	Transfer-Date	num	8	Transaction Set Creation Date
Time	Transfer-Time	num	8	Transaction Set Creation Time
Identification code	Rbha_id	char	2	RBHA Contractor ID
Reference Identification	group_bill_id/pr vider_id	char	9	Group Biller ID/Provider Id
Reference Identification	provider_id	char	9	Provider ID
Identification code	client-id	char	10	Client ID
Claim submitter's Identifier	ICN-Nbr	char	11	ICN Number
Monetary Amount	Billed_Amount	num	7	Line Item Charge Amount
Facility Code Value	Place_of_Service	char	2	Place of Service
Claim Frequency Type Code	Adjustment_Flag	char	1	"1"
Reference Identification	Prior_Auth_nbr	char	6	Prior Authorization Number
Reference Identification	Adjustment_icn	char	11	Claim Original Reference Number
Description	Dup-Override- Ind, Oth-Ins-Cov- Flag + Encounter- Processed-Date	char	10	String the three fields into a single 10 char entry
Industry Code	Diagnosis_code	char	5	Diagnosis Code
Industry Code	icd9_code_2	char	6	ICD9 code 2
Industry Code	icd9_code_3	char	6	ICD9 code 3
Industry Code	icd9_code_4	char	6	ICD9 code 4
Monetary Amount	Medicare_ payment	num	8	Medicare Payment
Monetary Amount	Medicare_allow_ amount	num	8	Medicare Allowed Amount
Monetary Amount	Medicare_ deductible	num	8	Medicare Deductible Amount
Monetary Amount	Other_ins_ payment	num	8	Other Insurance Payment
Assigned Number	Line_nbr	num	2	Line Number
Product/Service ID	Proc_code	char	5	Procedure Code
Procedure Modifier	Proc_Code_modif ier	char	2	Procedure Code Modifier
Monetary Amount	Billed_Amount	num	7	Line Item Charge Amount
Quantity	Unit_Of_Service	num	7	Unit of Service
Facility Code Value	place_of_svc	char	2	Place of Service
Date Time Period	Service-Start- Date, Serv-End Date	num	16	Service Date - End Date
Contract Type Code	svc-type	char	1	"05" or "02"
Monetary Amount	special-net- value/net-paid	num	7	Special Net Value or Net-Paid
Number of Included Segments	Transfer-Record- Count	num	8	Total # of segments (including ST and SE)

Table/Extract: Encounter NCPDP Data

Description:

All consumers who receive service through the RBHA system must have current identifying data in the ADHS/DBHS CIS. NCPDP Universal Pharmacy Claims/Encounters billing data are potentially time-sensitive and should reflect current identifying data and other consumer status items.

Purpose/Uses:

This file is used to send the form C (Pharmacy) Claims to CIS for approval. These claims are approved at CIS on a monthly basis and are subsequently transmitted to AHCCCS for approval.

** Denotes modification or exclusion of the field – see Description /Exclusion.*

CIS	ComCoTec	Data Type	Length	Description/Exclusions	Logic
Client_ID	Mbrid	varchar	18	Consumer ID	
NABP_ID	PharmID	int	4	Pharmacy ID	
Service_Start_Date(ccyymmdd)	SbmDte Filled	datetime	8	Date service starts	
Dispense_Quantity	SbmMetric Quant	int	4	Metric quantity dispensed	
NDC_Code1	NDCLabeler	char	5	Label	
NDC_Code2	NDCProduct	char	4	Product	
NDC_Code3	NDC Package	char	3	Package	
Prescription_Cost	AppDue	money	8	Cost of prescription	
Rx_Order_Date	DateRx Written (ccyymmdd)	datetime	8	Date of prescription	
ICN_Nbr *	ICN_Nbr	varchar	11	RxI ICN Number	2+YYJJJ (Submission Date)+'C'+NNNN

Stored Tables

Table/Extract: dbo.enrmass - Consumer Enrollment Master File

Description:

The Enrollment Master File is used for Arizona only. It captures data about a consumer's initial enrollment date, demographics, medical history/medication and some special population data. An enrollment record must exist in ENRMAS before records can be added to other files.

Purpose/Uses:

This file includes descriptive consumer demographics used in the development of all consumer demographic reporting. The data is used to better satisfy current needs and anticipate future needs of the ValueOptions' consumer groups. ENRMAS is used to store the data for the 834 (intake extract) and Demographics file. The table is used for reporting purposes to identify the number of consumers who are currently enrolled in ValueOptions. This table is also used as a reporting tool to identify consumers' demographics and enrollment information.

Name	Data Type	Length	Description
Lstnam	varchar	15	Last Name
Fstnam	char	10	First Name
Midnam	char	1	Middle Name
Membno	char	15	Consumer Number
Enrdat	int	4	Enrollment Date
Provid	char	7	CIS Provider ID Number
Refdat	int	4	Referral Date
Nendat	int	4	New Enrollment Date
Accsid	char	9	AHCCCS ID Number
Tempno	char	15	Temporary Consumer Number
Socsec	char	10	Social Security Number
adrln1	varchar	25	Address Line 1
adrln2	varchar	25	Address Line 2
Citycd	char	20	City
Stacod	char	2	State

Name	Data Type	Length	Description
ZIPcode	char	10	ZIP Code
County	char	2	County of Residence
Prires	char	2	Primary Residence Code
Bthdat	int	4	Birth Date
Sexcod	char	1	Gender
Hltpln	char	6	AHCCCS Health Plan ID
Racecd	char	2	Race Code
Ethcod	char	2	Ethnicity Code
Marsta	char	1	Marital Status
Refsrc	char	2	Referral Source
Priprb	char	2	Primary Presenting Problem
Pmtsrc	char	2	Payment Source
Othagy	char	1	Other Agency
medin1	char	1	Other Medical Insurance - 1st
medin2	char	1	Other Medical Insurance - 2nd
medin3	char	1	Other Medical Insurance - 3rd
Smised	char	1	Special Population - SMI/SED
spalc	char	1	Special Population - Alcohol User
spdrug	char	1	Special Population - Drug User
spmhth	char	1	Special Population - General Mental Health
spsped	char	1	Special Population - Special Education
spivdg	char	1	Special Population - IV Drug User
sppreg	char	1	Special Population - Pregnant
spwdech	char	1	Special Population - Woman w/Dependent Child
othpop	char	2	Special Population - Other
rbhafs	char	1	RBHA Funding Source Program Indicator
sysdat	int	4	System Date
lstchg	int	4	Last Change Date
cissdt	int	4	Date First Sent to CIS
cisrdt	int	4	Date Resent to CIS
cisadt	int	4	Date Accepted by CIS
cisudt	int	4	Date Updated by CIS
cisidt	int	4	Date Imported by CIS
cisedt	int	4	Date Error Imported by CIS
cissta	char	1	CIS Status Code
userad	char	10	User Who Added Record
userid	char	10	User Who Modified Record
cdcsdt	int	4	Date Sent to Cedar Client
cdcrdt	int	4	Date Resent to Cedar Client
cdستا	char	1	Cedar Status Code Client
cdesdt	int	4	Date Sent to Cedar Enrollment
cdcrdt	int	4	Date Resent to Cedar Enrollment
cdستا	char	1	Cedar Status Code Enrollment
cdbsdt	int	4	Date Sent to Cedar Brief
cdbrdt	int	4	Date Resent to Cedar Brief
cdbستا	char	1	Cedar Status Code Brief
delflg	char	1	Deleted Record Flag

Name	Data Type	Length	Description
cisfil	char	10	CIS Extract Filename
cdrfil	char	10	Cedar Extract Filename
mhsprv	char	15	MHS Provider Number
natttrt	char	1	Nature of Treatment/Legal Status
incarc	char	1	Incarceration Status
withid	char	1	Withdrawal Indicator
medmgt	char	1	Medication Management (Y/N)
meddat	int	4	Medication Management Date
rendisdat	char	8	Closure Date for CIS Intake Record
rcnasmdat	char	8	Assessment Date from CIS Intake Record
rcnsmi	char	1	SMI for Recon
rcnsed	char	1	SED for Recon
asmsmi	char	1	Assessment SMI for Recon
asmsed	char	1	Assessment SED for Recon
asmivdg	char	1	Assessment IV Drug for Recon
asmpreg	char	1	Assessment Pregnant for Recon
asmwdch	char	1	Assessment Woman w/Dependent Child for Recon
securid	num	7	Corporate Security ID
srvcenid	char	2	Service Center ID
filgrp	char	1	File Group

Table/Extract: dbo.sppmas -

Description:

This file contains the Consumer Enrollment Extension File specific to Arizona. The Consumer Enrollment Extension File is closely related to ERMAS (Enrollment). The file contains descriptive consumer demographics used in the development of all consumer demographics.

Purpose/Uses:

The data are used to better satisfy current needs and to anticipate future needs of ValueOptions' consumers. The data from this file also supports a variety of activities including: Disenrollment, Comprehensive Assessment, and Special Population in addition to Enrollment.

Name	Data Type	Length	Description
lstnam	varchar	15	Last Name
fstnam	char	10	First Name
midnam	char	1	Middle Name
membno	char	15	Consumer Number
enrdat	int	4	Enrollment Date
begdat	int	4	Begin Date
enddat	int	4	End Date
stargate	char	1	Stargate Indicator (Y/N)
title36	char	1	Title 36 Indicator (Y/N)
coolp200	char	1	Cool Prop Indicator (Y/N)
collafcare	char	1	Cool After Care Indicator (Y/N)
collgenpar	char	1	Cool Gen Parole Indicator (Y/N)
userad	char	10	User Who Added Record
sysdat	int	4	System Date

Name	Data Type	Length	Description
userid	char	10	User Who Last Modified Record
lstchg	int	4	Last Change Date
modflag	char	1	Modified Flag (Y/N)
securid	numeric	7	Corporate Security ID
srvcenid	char	2	Service Center ID
filgrp	char	1	File Group

Table/Extract: dbo.dismas - Consumer Disenrollment Master File

Description:

The Consumer Disenrollment Master File captures disenrollment data for consumers, including items such as: enrollment/disenrollment dates, disenrollment reason and basic consumer data. This file captures additional data not captured on C.O.O.L., sub groups and corporate security ID.

Purpose/Uses:

This file is used to create the 834 Closure and Demographics File. This file is used to report on which consumers are closed in the RBHA. This table is used to store disenrollment information such as problem resolution, disenrolling reason and whether or not the consumer was transferred to another provider for other services.

Name	Data Type	Length	Description
membno	char	15	Consumer Number
Enrdat	int	4	Enrollment Date
Disdat	int	4	Disenrollment Date
typmov	char	1	Type of Movement
Disrsn	char	2	Disenrollment Reason
Svctfr	char	2	Service Center From
Resprb	char	1	Resolution of Problem
Accsid	char	9	AHCCCS ID Number
socsec	char	10	Social Security Number
Lstnam	varchar	15	Last Name
Fstnam	char	10	First Name
midnam	char	1	Middle Name
Bthdat	int	4	Date of Birth
Provid	char	7	CIS Provider ID
Sysdat	int	4	System Date
Lstchg	int	4	Last Change Date
Cissdt	int	4	Date First Sent to CIS
Cisrdt	int	4	Date Resent to CIS
Cisadt	int	4	Date Accepted by CIS
Cisudt	int	4	Date Updated by CIS
Cisidt	int	4	Date Imported by CIS
Cisedt	int	4	Date Error Imported by CIS
Cissta	char	1	CIS Status Code
Cdrsdtd	int	4	Date First Sent to Cedar
userad	char	10	User Who Added the Record
Userid	char	10	User Who Modified the Record
Cdrrdt	int	4	Date Resent to Cedar
Cdrsta	char	1	Cedar Status Code

Name	Data Type	Length	Description
Delflg	char	1	Deleted Record Flag
Cisfil	char	10	CIS Extract Filename
Cdrfil	char	10	Cedar Extract Filename
securid	numeric	7	Corporate Security ID
svrcenid	char	2	Service Center ID
Filgrp	char	1	File Group

Table/Extract: dbo.cmpmas

Description:

The Comprehensive Consumer Assessment File captures consumer assessment data, including elements such as: household size, income, agencies involved with consumer, substance abuse data and brief medical history.

Purpose/Uses:

This file is used to create the demographic extract to the state and also to create reports for providers and internal staff. This data supports reporting on specific consumer demographics, education, employment, and medical history.

Name	Data Type	Length	Description
membno	char	15	Consumer Number
Enrdat	int	4	Consumer Enrollment Date
asmdat	int	4	Consumer Assessment Date
Provid	char	7	CIS Provider ID Number
Assint	char	1	Assessment Interval
nasdat	int	4	New Assessment Date
ispcmp	char	1	ISP Completed
Ispcdt	int	4	ISP Completion Date
hincom	int	4	Household Income
Hsize	smallint	2	Household Size
Isafdc	char	1	Income Source - AFDC/TANF
Isemp	char	1	Income Source - Employment
Isfam	char	1	Income Source - Family
Isfstp	char	1	Income Source - Food Stamps
Isgast	char	1	Income Source - Gen Assistance
isnone	char	1	Income Source - None
Isoth	char	1	Income Source - Other
Isret	char	1	Income Source - Retirement
Isss	char	1	Income Source - Social Security
Issdi	char	1	Income Source - SSDI
Isssi	char	1	Income Source - SSI
isuemp	char	1	Income Source - Unemployment
Isvet	char	1	Income Source - Veteran Comp
Nattrt	char	1	Nature of Treatment - Legal Stat
agadjc	char	1	Agencies - AZ Dept of Juvenile Correct
Adcjp	char	1	Agencies - Courts/Juvenile Probation
Adcap	char	1	Agencies - Adult Probation
agacyf	char	1	Agencies - Asst Child/Youth/Family
Agddd	char	1	Agencies - DIV DEV Disabilities

Name	Data Type	Length	Description
Agdvr	char	1	Agencies - DIV VOC Rehab
Agdc	char	1	Agencies - Department of Corrections
empsta	char	2	Employment Status
Edstat	char	1	Education Status
schyrs	char	3	Formal School Years Completed
Arrest	char	4	Number of Arrests in Past Year
Sbtyp1	char	4	Substance Type 1st
Sbfrq1	char	1	Substance Frequency 1st
sbrte1	char	1	Substance Route 1st
Sbage1	smallint	2	Substance Age Used 1st
Sbtyp2	char	4	Substance Type 2nd
Sbfrq2	char	1	Substance Type 2nd
sbrte2	char	1	Substance Frequency 2nd
Sbage2	smallint	2	Substance Route 2nd
Sbtyp3	char	4	Substance Type 3rd
Sbfrq3	char	1	Substance Frequency 3rd
sbrte3	char	1	Substance Route 3rd
Sbage3	smallint	2	Substance Age Used 3rd
cmarth	char	1	CRN MED DO - Arthritis
cmasma	char	1	CRN MED DO - Asthma/COPD
cmcncr	char	1	CRN MED DO - Cancer
cmdiab	char	1	CRN MED DO - Diabetes
cmhdin	char	1	CRN MED DO - Head Injury
cmhdac	char	1	CRN MED DO - Headache
cmhbp	char	1	CRN MED DO - High Blood Pressure
Cmoth	char	1	CRN MED DO - Other
Cmhrt	char	1	CRN MED DO - Heart/Cardio Disease
Cmszr	char	1	CRN MED DO - Seizures
Dsma1p	char	6	DSMIV Code Axis I Principle
Dsma1a	char	6	DSMIV Code Axis I Additional
Dsma2p	char	6	DSMIV Code Axis II Principle
Dsma2a	char	6	DSMIV Code Axis II Additional
Dsma3	char	6	DSMIV Code Axis III
Alfarp	char	3	ALFA Role Performance
Alfasc	char	3	ALFA Self Care/Living Skills
Alfasl	char	3	ALFA Social/Legal
Alfair	char	3	ALFA Interpersonal Relationships
Alfasu	char	3	ALFA Substance Abuse
Alfafl	char	3	ALFA Family/Living Environment
Alfatc	char	3	ALFA Thinking/Cognition
Alfafm	char	3	ALFA Feel/Affect/Mood
alfamp	char	3	ALFA Medical/Physical
cgisev	char	2	CGI Severity of Symptoms
cgiimp	char	2	CGI Global Improvement
Cgieff	char	3	CGI Efficacy Index
sf1201	char	2	SF12 Health Survey - Question 1
sf1202	char	2	SF12 Health Survey - Question 2

Name	Data Type	Length	Description
sf1203	char	2	SF12 Health Survey - Question 3
sf1204	char	2	SF12 Health Survey - Question 4
sf1205	char	2	SF12 Health Survey - Question 5
sf1206	char	2	SF12 Health Survey - Question 6
sf1207	char	2	SF12 Health Survey - Question 7
sf1208	char	2	SF12 Health Survey - Question 8
sf1209	char	2	SF12 Health Survey - Question 9
sf1210	char	2	SF12 Health Survey - Question 10
sf1211	char	2	SF12 Health Survey - Question 11
sf1212	char	2	SF12 Health Survey - Question 12
sysdat	int	4	System Date
Lstchg	int	4	Last Change Date
Cissdt	int	4	Date First Sent to CIS
Cisrdt	int	4	Date Resent to CIS
Cisadt	int	4	Date Accepted by CIS
Cisudt	int	4	Date Updated by CIS
Cisidt	int	4	Date Imported by CIS
Cisedt	int	4	Date Error Imported by CIS
Cissta	char	1	CIS Status Code
userad	char	10	User Identification - Add
Userid	char	10	User Identification - Change
cdrsdt	int	4	Date First Sent to Cedar
Cdrrdt	int	4	Date Resent to Cedar
Cdrsta	char	1	Cedar Status Code
Delflg	char	1	Deleted Record Flag
Cisfil	char	10	CIS Extract Filename
Cdrfil	char	10	Cedar Extract Filename
Smiflg	char	1	SMI Indicator
Sedflg	char	1	SED Indicator
spivdg	char	1	SPEC POPS - IV Drug User
sppreg	char	1	SPEC POPS - Pregnant
spwdch	char	1	SPEC POPS - Woman w/Dependent Child
securid	numeric	7	Corporate Security ID
srcenid	char	2	Service Center ID
Filgrp	char	1	File Group

Table/Extract: dbo.tblRxIData

Description:

This data is comprised of the service records of consumer, physician, and pharmacy at the prescription level of detail. The data management is outsourced to ComCoTec. ComCoTec performs pharmacy claims processing and servicing functions. The file is downloaded from the FTP web server on a weekly basis and is loaded into the data warehouse.

Purpose/Uses: Pharmacy Table:

This file is used to create the extract (NCPDP) file to the CIS System. The data is used for medical quality management by tracking drug utilization and cost. The data identifies the pharmacy, consumer, and drug, and is used as a reference to verify pharmacy claims. The data is the source for reports on a variety of topics including Consumer Prescription Activity, Physician Prescription Activity, Pharmacy Prescription Service Activity, Drug Utilization, Internal Accounting, Medical Quality Management, Pharmacy Drug Utilization and Claim Activity.

tblRxIData and AHCCCS_NABP_ID from Rx_Data database

Name	Data Type	Length	Description
CarrierId	varchar	9	Carrier ID
SbmDteFilled	datetime	8	Service Date
DateSubmitted	datetime	8	Submission Date
TCDClaimStatus	varchar	1	Claim Type
ClaimCounter	smallint	2	Claim Flag
MbrID	varchar	18	RxI Number
AccountID	varchar	15	Account ID
GroupID	varchar	15	Group ID
FinalPlanCode	varchar	10	Final Plan Code
PlanDrugStatus	varchar	1	Plan Drug Status
RxNbr	int	4	RxI Nbr Number
RxClaimNbr	varchar	15	RxI Claim Number
RxClaimSeqNbr	smallint	2	RxI Claim Seqnumber
DateRxWritten	datetime	8	RxI Written Date
DrugLabelName	varchar	25	Drug Label Name
DrugLabelNameOriginal	varchar	25	Original Drug Label Name
DrugStrength	int	4	Drug Strength
DrugGenericName	varchar	60	Drug Generic Name
DrugGenericNameOriginal	varchar	60	Original Drug Generic Name
DrugGenStrength	int	4	Drug Generic Strength
SbmMetricQuant	int	4	Dispense Quantity
SbmNewRefillCode	int	4	Refill Code
SbmDaysSupply	int	4	Days Supply
AWPUnitCost	money	8	Average Wholesale Price Unit Cost
GenericIndMedispan	varchar	1	Multi-source Code
GenericIndOverride	varchar	1	Multi-source Override
SbmCompoundCode	int	4	Sbm Compound Code
SbmMaxRefills	int	4	Sbm Nbr Refills Authorized
SbmLevelOfSvc	int	4	Sbm Level of Service
SbmProdSelectCode	int	4	Sbm Prod Select Code
SbmCustLoc	int	4	Sbm Customer Location
ReimbursementFlag	varchar	1	Reimbursement Flag
CareFacility	varchar	6	Care Facility ID
CareFacilityName	varchar	25	Care Facility Name
GPINbr	varchar	14	GPI Number
GPI2	varchar	2	GPI Number 2
GPI4	varchar	4	GPI Number 4
GPI6	varchar	6	GPI Number 6
GPI8	varchar	8	GPI Number 8
GPI10	varchar	10	GPI Number 10
GPI12	varchar	12	GPI Number 12
NDCLabeler	int	4	NDC Labeler ID
NDCProduct	int	4	NDC Product ID

Name	Data Type	Length	Description
NDCPackage	int	4	NDC Package ID
AppDue	money	8	Prescription Cost
AppCopay	money	8	Approved Copay Amt
AppDispFee	money	8	Approved Disp Amt
AppIngredCost	money	8	Approved Copay Amt
AppSalesTax	money	8	Approved Attributed to Sales Tax Amt
AppPatientPay	money	8	Approved Patient Payment
AppWithholdAmt	money	8	Approved Withhold Amt
MbrLastName	varchar	25	Consumer Last Name
MbrFirstName	varchar	15	Consumer First Name
MbrMidInit	varchar	1	Consumer Initial
MbrDOB	datetime	8	Consumer DOB
MbrSex	varchar	1	Consumer Gender
MbrZIP	varchar	10	Consumer ZIPcode
MbrCalcAge	int	4	Consumer Age
HEDISAgeBand	varchar	1	HEDIS Age Band
PrescID	varchar	10	Prescription ID
PrescLastName	varchar	25	Prescription Last Name
PrescFirstName	varchar	15	Prescription First Name
PrescSpecialtyCode	varchar	6	Prescription Specialty Code
PrimaryPrescID	varchar	10	Primary Presc ID
PrimaryPrescLastName	varchar	25	Primary Presc Last Name
PrimaryPrescFirstName	varchar	15	Primary Presc First Name
PrimaryPrescSpecCode	varchar	6	Primary Presc Special Code
PharmID	int	4	Pharmacy ID
PharmName	varchar	25	Pharmacy Name
PharmZIP	int	4	Pharmacy ZIPcode
PharmNetworkID	varchar	6	Pharmacy Network ID
PharmNetworkName	varchar	25	Pharmacy Network Name
PharmPayCenter	int	4	Pharmacy Pay Center
PharmAffiliationCode	varchar	9	Pharmacy Affiliation Code
PostAdjDueAmt	money	8	Post Adj Due Amount
PostAdjCopayAmt	money	8	Post Adj Copay Amt
PostAdjDispFee	money	8	Post Adj Disp Fee
PostAdjIngredCostPaid	money	8	Post AdjIngred Cost Paid
PostAdjSalesTaxPaid	money	8	Post Adj Sales Tax Paid
PostAdjPatientPaidAmt	money	8	Post Adj Patient Paid Amt
PostAdjWithholdAmt	money	8	Post Adj Withhold Amt
PostAdjSelAmt	money	8	Post Adj Sel Amt
PostAdjIncentFee	money	8	Post AdjIncent Fee
PostAdjCostSource	varchar	1	Post Adj Cost Source
PostAmtAttribToDed	money	8	Post Amt Attrib To Ded
PostExePerBftAmt	money	8	Post Exe Per Benefit Amt
CostTypeUnitCost	money	8	Cost Type Unit Cost
CostTypeCode	varchar	10	Cost Type Code
DrugManufacturer	varchar	10	Drug Manufacturer
DrugDosageForm	varchar	4	Drug Dosage Form

Name	Data Type	Length	Description
DrugAdminRoute	varchar	2	Drug Admin Route
DrugUnitDosePerU	varchar	1	Drug Unit Dose Per U
Drug3rdPartyExcep	varchar	1	Drug 3 rd Party Excep
DrugDEACode	varchar	1	Drug DEA Code
DrugFDATheraEquiv	varchar	2	Drug FDA Thera Equiv
DrugRxOTCInd	varchar	1	Drug Rx OTC Ind
SbmUsualAnd Customary	money	8	Sbm Usual And Customary
SbmIngredCost	money	8	Sbm Ingred Cost
SbmSalesTax	money	8	Sbm Sales Tax
SbmDispFee	money	8	Sbm Disp Fee
SbmGrossAmtDue	money	8	Sbm Gross Amount Due
SbmPatientPaidAmt	money	8	Sbm Patient Paid Amount
AppAtrProdSelAmt	money	8	Approved Atr Prod Sel Amount
AppIncentiveFee	money	8	Approved Incentive Fee
AppAdminAmt	money	8	Approved Admin Amt
AppCostSource	varchar	1	Approved Cost Source
AppAmtAttribToDed	money	8	Approved Amount Attrib To Ded
AppExcePerBftAmt	money	8	Approved Exce Per Benefit Amount
RevLevelOfService	varchar	2	Rev Level Of Service
RevIncentiveAmtPaid	money	8	Rev Incentive Amount Paid
RevIncentiveFeePd	money	8	Rev Incentive Fee Paid
RevDateSbm	datetime	8	Rev Date Sbm
RevDURConflictCode	varchar	2	Rev DUR Conflict Code
RevDURIntervenCode	varchar	2	Rev DUR Interven Code
RevDUROutcomeCode	varchar	2	Rev DUR Outcome Code
SbmDURConflictCode	varchar	2	Sbm DUR Conflict Code
SbmDURIntervenCode	varchar	2	Sbm DUR Interven Code
SbmDUROutcomeCode	varchar	2	Sbm DUR Outcome Code
DURKey	varchar	18	DUR Key
DrugConflictCode	varchar	2	Drug Conflict Code
SeverityIndexCode	varchar	1	Severity Index Code
OtherPharmacyInd	varchar	1	Other Pharmacy Ind
DateOfPrevFill1	datetime	8	Date Of Prev Fill 1
QtyOfPrevFill1	int	4	Quantity Of Prev Fill 1
DatabaseInd1	varchar	1	Database Ind 1
OtherPrescriberInd1	varchar	1	Other Prescriber Ind 1
FreeText1	varchar	30	Free Text 1
DrugConflictCode2	varchar	2	Drug Conflict Code 2
SeverityIndexCode2	varchar	1	Severity Index Code 2
OtherPharmacyInd2	varchar	1	Other Pharmacy Ind 2
DateOfPrevFill2	datetime	8	Date Of Prev Fill 2
QtyOfPrevFill2	int	4	Quantity Of Prev Fill 2
DatabaseInd2	varchar	1	Database Ind 2
OtherPrescriberInd2	varchar	1	Other Prescriber Ind 2
FreeText2	varchar	30	Free Text 2
DrugConflictCode3	varchar	2	Drug Conflict Code 3
SeverityIndex3	varchar	1	Severity Index 3

Name	Data Type	Length	Description
OtherPharmacyInd3	varchar	1	Other Pharmacy Ind 3
DateOfPrevFill3	datetime	8	Date Of Prev Fill 3
QtyOfPrevFill3	int	4	Qty Of Prev Fil l3
DatabaseInd3	varchar	1	Database Ind 3
OtherPrescriberInd3	varchar	1	Other Prescriber Ind 3
FreeText3	varchar	30	Free Text 3
RejectCount	int	4	Reject Count
RejectCode1	int	4	Reject Code 1
RejectCode2	int	4	Reject Code 2
RejectCode3	varchar	5	Reject Code 3
UserDefinedField1	varchar	10	User Defined Field 1
UserDefinedField2	varchar	10	User Defined Field 2
UserDefinedField3	varchar	10	User Defined Field 3
CCTDefinedField1	varchar	10	CCT Defined Field 1
CCTDefinedField2	varchar	10	CCT Defined Field 2
CCTDefinedField3	varchar	10	CCT Defined Field 3
DrugGroup	varchar	2	Drug Group
MbrPriorAuthRsn	varchar	11	Consumer Prior Authorization Reason
MbrPriorAuthNbr	varchar	11	Consumer Prior Authorization Reason Number
membno	char	15	CIS Consumer Number
accepted	char	1	'Y' = Accepted By State, 'N' = Not Accepted
ICN_Nbr	varchar	11	ICN Number of RxI Claim

Table/Extract: DW_Claims

Description:

The DW Claim table is a pre-joined table that includes data elements from several different sources pertaining to claims. The MHS AS/400 source tables used to populate this table are: AHDMA, CAPMA, DEMMA, MEDMA, MEMMA, MEXMA and PRVMA. The primary key for DW_CLAIM consists of the following fields: braned, batdat, batseq, seqnum and linenum. Together, these fields make the internal batch number for unique identification.

Purpose/Uses:

This is used as the central repository for all claims data used in reporting. The file is the primary source for all claims and financial reporting for use internally and externally. The data is also used for quality management purposes. The data identifies the Claims, Consumers and Providers and is used as a reference to verify claims. This information is also used to verify legitimate claims by identifying consumers and providers.

Name	Data Type	Length	Description
id_claim	int	15	Relative Record Number
braned	char	4	Branch Code
batdat	int	8	Batch Date
batseq	int	10	Batch Sequence Number
seqnum	int	15	Sequence Number
linenum	int	2	Line Number
vendor	char	15	Vendor Number
chknum	num	10	Check Number
athbrn	char	4	Authorization Branch Code
athbat	int	8	Authorization Batch Date
athseq	int	10	Authorization Batch Sequence Number

Name	Data Type	Length	Description
athnum	int	15	Authorization Sequence Number
compno	smallint	4	Company Number
grpnum	char	6	Group Number
stated	char	1	Status Code
provno	char	15	Provider Number
membno	char	15	Consumer Number
svcdat	int	8	Date of Service
svccod	char	6	Medical Service Code
modcod	char	2	First Service Code Modifier
modcd2	char	2	Second Service Code Modifier
modcd3	char	2	Third Service Code Modifier
modcd4	char	2	Fourth Service Code Modifier
pepcod	char	15	Primary Care Physician Code
enddat	int	8	Ending Service Date
unitct	smallint	4	Unit Count
poscod	char	2	Place of Service code
toscod	char	2	Type of Service Code
diagn1	char	8	Diagnosis 1
diagn2	char	8	Diagnosis 2
claamt	money	16	Claimed Amount
alwamt	money	16	Allowed Amount
copamt	money	16	Co-payment Amount
whdamt	money	16	Withhold Amount
dscamt	money	16	Discount Amount
nonamt	money	16	Non-covered Amount
preamt	money	16	Prepaid Amount
dedamt	money	16	Deductible Amount
cobamt	money	16	COB (Coordination of Benefits) Amount
rcvamt	money	16	COB Savings Amount
glcode	char	4	GL Code
pidate	int	8	Paid Date
athtyp	char	1	Authorization Type
clatyp	char	2	Claim Type Code
prvcpy	char	2	Provider Capacity Code
paycod	char	1	Payment Code
fndtyp	char	2	Fund Type
coiamt	money	16	Coinsurance Amount
lstchg	int	8	Last Change Date
feecod	char	6	Fee Code
alwunt	int	4	Allowed Units
formcd	char	1	Forms Code
athlin	int	15	Authorization Line Number
edtdat	int	8	Edit Date
rcvdat	int	8	Received Date
sysdat	int	8	System Date
bencod	char	3	Benefit Code
benpkg	char	4	Benefit Package
prvorg	char	4	Provider Organization Code
userid	char	10	User Identification
topay	money	16	To-Pay Amount
claimno	char	22	Claim Number

Name	Data Type	Length	Description
inscod	char	3	Insurance Company Code
apthbat	num	11	Batch Number
aptseq	int	15	Sequence Number
tiercd	char	4	Tier Level Code
diagn3	char	8	Diagnosis 3
conset	smallint	15	Contract Sequence Number
ovrcod	char	1	Override Code
edtcod	char	3	Service Edits Code
prccod	char	1	Process Indicator
patamt	money	16	Amount Patient Has Paid
procod	char	3	Banking Profile Code
clmsc	char	4	Claim Service Center
pstdat	int	8	Posting Date
origpd	int	8	Original Paid Date
origchk	numeric	10	Original Check Number
admdat	int	8	Admission Date
disdat	int	8	Discharge Date
bthdat	int	8	Date of Birth
sexcod	char	1	Gender
racecd	char	1	Race Code
icmflag	char	1	Intensive Case Management Flag
ZIPcod	char	10	ZIP Code
lstnam	varchar	20	Consumer's Last Name
fstnam	char	15	Consumer's First Name
midnam	char	1	Consumer's Middle Initial
relcod	char	1	Relationship Code
subsno	char	15	Subscriber Number
prvnam	varchar	36	Provider Name
titled	char	4	Provider's Title Code
prvtyp	char	2	Provider Type
prvZIPcod	char	10	Provider ZIP Code
county	char	2	County of Residence
parent	char	4	Parent/Client Code
memage	int	3	Consumer's Age
cpaicn	char	16	Claims Internal Control Number
socnam	varchar	35	Source of Care Description
payvendor	char	15	Pay-To Vendor
hosbeg	int	8	Hospital Beginning Date
hosend	int	8	Ending Date
bilcod	char	3	Bill Type Code
patnum	char	38	Patient Number
altprv	char	15	Alternate Provider Number
refphy	varchar	30	Provider's Social Security Number
faccod	varchar	35	Facility Code
admtyp	char	1	Admission Type
admsrc	char	1	Admission Source
patsta	char	2	Patient Discharge Status
submid	char	16	EDI Submitter ID
mex_admdat	int	8	MEXMAS Admission Date
svccenid	char	2	Service Center ID
filgrp	char	1	File Group

Table/Extract: dbo.AHCCCS_NABP_ID

Description:

The file contains Provider information such as name, address, phone number and licensing information. The data is provider-specific for internal and external reporting. After creating the file, an update is performed (Update NABP_ID = AHCCCS + '01' and Group_Biller_ID = AHCCCS) by Joining NABP_ID to the field of NABP_ID of AHCCCS_NABP_ID table.

Purpose/Uses:

This file is used to crosswalk the Pharmacy's NABP ID to the AHCCCS ID. ValueOptions uses this file to verify the provider and pharmacy activity against all the criteria required by AHCCCS. ValueOptions checks to ensure provider licensing is valid and current.

Name	Data Type	Length	Description
PROVNUM	sysname	9	CIS Provider Number
AHCCCS	sysname	6	Access Provider#
PROVNAME	varchar	50	CIS Provider Name
ADDRESS1	varchar	50	Address of Provider
CITY	sysname	18	City of Provider
STATE	sysname	2	State of Provider
ZIP	sysname	6	ZIPcode of Provider
PHONE	sysname	11	Phone of Provider
HS_TYPE	sysname	2	Type of HS
AH_TYPE	sysname	2	Type of AH
LICENSE	sysname	10	License
STARTDATE	datetime	8	Starting Date
ENDDATE	datetime	8	Ending Date
NABP_ID	sysname	10	NABP Identification
OLD_NABP_ID	sysname	10	Old NABP Identification
NABP_ID_Int	int	4	NABP Identification Integer
SYSDATE	datetime	8	System Date

Table/Extract: tblCOOLConsumers (Source from COOL (The Correctional Officer/Offender Liaison Program))

Description:

The Correctional Officer/Offender Liaison (COOL) Program was established to better serve the substance abuse and behavioral health service needs of high-risk offenders on parole from the Arizona Department of Corrections. This table is used for updating the flag "SF_COOL" of the Demographic table to 'Y' for indicating a COOL consumer.

Mapping Tables: By ClientID to membno of ENRMAS table and DateDischargedFrProv or SupervisionEndDt Greater than or Equal to Today's Date

Purpose/Uses:

The data from this file supports the reporting functions for the roster for COOL groupings. ValueOptions uses this file to verify that the services for our consumers meet all the criteria required by the COOL guidelines.

Name	Data Type	Length	Description
ReferralID	int	4	Referral ID for <u>internal use only</u>
ClientID	int	4	Client ID for <u>internal use only</u>

Name	Data Type	Length	Description
MHSID	varchar	15	Consumer ID
MHSID_Orig	varchar	15	Original Consumer ID for <u>internal use only</u>
ADCNum	varchar	10	Parole AZ Dept of Corrections Number
SSN	varchar	11	Social Security Number
Gender	varchar	1	Gender
DateRefRecd	datetime	8	Referral Date From Parole Officer
IntakeDate	datetime	8	Intake Date From Provider
DateOfProvRef	datetime	8	Date COOL Referred Parolee to Provider Either over the Phone, Mail or Fax.
DateDischargedFrProv	datetime	8	Date Provider Discharged Parolee from Referred Services
SupervisionEndDt	datetime	8	Supervision End Date from ValueOptions
NatureOfDischarge	varchar	50	Reason Parolee was discharged from provider
MHSProv	varchar	15	MHS Provider Number
ClaimProvName	varchar	50	MHS Provider Name
CoolProvId	int	4	COOL Provider ID for <u>internal use only</u>

Table/Extract: HB_Roster_Main

Description:

This table stores the House Bill 2003 roster for both child and adolescent and adult groupings. The table is keyed from the Consumer's CIS ID and the House Bill Identification date. Data is pulled from this roster for the purpose of sending a House Bill 2003 roster to the State on a monthly basis. The data in this table includes more information than the minimum required by the State.

Purpose/Uses:

The data from this file supports the reporting functions for the roster for both child and adolescent, and adult groupings. ValueOptions uses this file to verify that the services for our consumers meet all the criteria required by House Bill 2003.

Name	Data Type	Length	Description
CISID	nvarchar	10	Consumer Number
AHCCCSID	nvarchar	6	The AHCCCS ID Number identifies a unique consumer in the AHCCCS system
SSN	nvarchar	10	Social Security Number
LName	nvarchar	25	Last Name
FName	nvarchar	25	First Name
DOB	int	8	Date of Birth (ccyymmdd)
HBIdDat	int	8	Start Date
HBDisDat	int	8	Discontinuing Date
LastAsmtDat	int	8	Last Assessment Date(From CMPMAS table)
MultiAgy	nvarchar	25	Multiple Agencies
FirstHBSvcDat	int	8	First Service Date
FamId1	nvarchar	25	Family ID1
FamId2	nvarchar	25	Family ID2
FamId3	nvarchar	25	Family ID3
FamId4	nvarchar	25	Family ID4
FamId5	nvarchar	25	Family ID5
FamId6	nvarchar	25	Family ID6
FamId7	nvarchar	25	Family ID7

Name	Data Type	Length	Description
FamId8	nvarchar	25	Family ID8
FamId9	nvarchar	25	Family ID9
FamId10	nvarchar	25	Family ID10
Program	nvarchar	3	Program Type
ACT/Sup	nvarchar	50	Act Team or Supporting Team
PriorityClass	nvarchar	50	SMI Priority Class(1. ASH Clients, 2. Supervisor Clients, 3. Jail Clients, 4. 24hrs/Residential Clients, 5. Frequent Hospital User, 'Non-Priority'
RehabStatusCode	nvarchar	50	Rehabilitation Status Code
RehabCategory	nvarchar	50	Description of Rehabilitation Status Code
ErrorStatus	nvarchar	25	Error Status
ABSID	int	8	ABS ID for <u>Internal Use Only</u>
grpnum	nvarchar	50	Eligibility Group Number
Assign_Enr	nvarchar	50	First Enrollment Date
Current_Enr	nvarchar	50	Current Enrollment Date

Table/Extract: tblcapfile_ccyymm - BHS Capitation Detail File

Description:

The CAP file is currently received from the State of Arizona and is used as a reporting tool to identify potential consumers. The file is received from Arizona Department of Health Services on a monthly basis. This file is generally ready the first week of every month. The data from the file is loaded into the ValueOptions data warehouse where it is used for reports such as demographics, ZIP codes and potential target areas for consumers needing services.

Purpose/Uses:

BHS Capitation Detail File is received on the 1st of the month, and is uploaded into the Reporting Database on a monthly basis. The data supports penetration analysis and enables the analysis of ValueOptions current enrollment against total eligibles for Maricopa County. The file is used to identify potential and current consumers by ZIP code and other various reports.

Name	Data Type	Length	Description
Health Plan Identification Number	char	6	AHCCCS Health Plan
Ctrt Type	char	1	Certification Type
City Service Area Code	char	2	City Location
AHCCCS Identification Number	char	9	Consumers AHCCCS Id Number
Process Sequence Number	char	2	System Generated Sequence Number
Enrollment End Date	char	8	Consumers AHCCCS Eligibility End Date
Recipient Name	char	34	Consumers Name
Eligibility Key Code	char	3	Consumers Eligibility Key Code
ZIP Code	char	9	Consumers ZIP Code
Gender	char	1	Consumers Gender
Date of Birth	char	8	Consumers Date Of Birth
Enrollment Begin Date	char	8	Consumers AHCCCS Eligibility Begin Date
Payment Type	char	2	Capitation Payment Type
Payment Date	char	8	Capitation Payment Date
Payment From Date	char	8	Capitation Payment From Date
Payment To Date	char	8	Capitation Payment To Date

Name	Data Type	Length	Description
Payment Amount	char	11	Capitation Payment Amount
Payment Cycle	char	2	Capitation Payment Cycle
Voucher Identification Number	char	16	Tracking Number of Check
Capitation Rate Code	char	4	Capitation Rate Code
Date Received Added	char	8	Received Date
Last Modified Date	char	8	Date of Last Modification
Last Modified Time	char	8	Time of Last Modification
Last Modified User	char	8	Last System User to Make Modification
Act type - Y or N (Native American)	char	1	Native American Flag
Case Identification Number	char	9	AHCCCS Case Identification Number
Sta	char	1	Capitation Status
Capitation Days	char	3	Number Of Capitation Days
Acute Health Plan Identification Number	char	6	AHCCCS Health Plan
Tribe Code	char	2	Tribal Code
MH Category	char	1	Mental Health Category
Acute Enrollment Rate Code	char	4	AHCCCS Enrollment Rate Code

Table/Extract: TPL File (Third Party Liability)

Description:

The file is downloaded on a daily basis and is loaded into the ValueOptions data warehouse. The data contained in the file is the source for several reports, and is also used while processing claims to verify consumers marked as having “TPL” (Third Party Liability), and to verify the contents of specific fields.

Purpose/Uses:

This file/table is used to distinguish whether a consumer has Medicare. This file is loaded in the data warehouse on a daily basis, and is used to verify that a consumer has Medicare that is in effect.

Name	Data Type	Length	Description
SequenceNumber	int	15	Sequence number
ProcessDate	varchar	50	Process date
LastName	varchar	50	Last name
FirstName	varchar	50	First name
Gender	varchar	2	Gender
DateOfBirth	datetime	8	Date of birth
PolicyNumber	varchar	50	Policy number
CoverageType	varchar	1	Coverage Type
BeginDate	datetime	8	Begin date
EndDate	datetime	8	End date
CarrierName	varchar	50	Carrier name
CarrierPhone	varchar	50	Carrier phone number
CarrierStreetAddress1	varchar	50	Carrier street address line 1
CarrierStreetAddress2	varchar	50	Carrier street address line 2

Name	Data Type	Length	Description
CarrierCity	varchar	50	Carrier city
CarrierState	varchar	2	Carrier state
CarrierZIPcode1	varchar	5	Carrier ZIP code part 1
CarrierZIPcode2	varchar	4	Carrier ZIP code part 22
InsuredLastName	varchar	50	Insured last name
InsureFirstName	varchar	50	Insure first name
InsuredMiddleInitial	varchar	50	Insured middle initial
Relationship	varchar	1	Relationship
InsuredEmployer	varchar	50	Insured employer
InsuredGroupNumbe	varchar	50	Insured group number
DateRecordAdded	datetime	8	Date record added
DateLastModified	datetime	8	Date last modified
DateVerified	datetime	8	Date verified
healthPlanID	varchar	6	Health Plan ID

Table/Extract: AHCCCS Eligibility

Description:

The data from this file is uploaded into MHS and may be used to add, modify or terminate a consumer's eligibility.

Purpose/Uses:

This file is received daily from CIS and is used to add new segments of eligibility to MHS, delete segments that are no longer valid, and terminate current records that are now closed. ValueOptions uses this file to build the eligibility file in MHS titled MEMMAS. MEMMAS is used to distinguish the group to which the consumer is assigned and the benefit package for which the consumer is eligible.

Name	Data Type	Length	Description
Transaction Type	char	1	'A' = Add, 'C' = Change, 'D' = Delete
Transaction Sequence Code	num	2	Sequence Code Number
AHCCCS ID	char	9	Consumers AHCCCS ID
Start Date	char	8	Consumers AHCCCS Effective Date
End Date	char	8	Consumers AHCCCS Expiration Date
Client ID	char	10	CIS Client Id
MHS Category	char	1	Mental Health Category
Capitation Code	char	4	Capitation Rate Code
Contract Type	char	1	Consumers Contract Type
Change Control Date	char	8	Date Record Was Last Changed
Change Control User Identification	char	30	Program That Last Changed Record
CIS Add Date	char	8	Date Added To CIS
Change Control Program	char	8	Change Control Program
Contractor Identification Number	char	2	Contractor Identification Number

Table/Extract: State Roster

Description:

The file is received daily from the Arizona Department of Health Services. There is also a full refresh file each Monday. The data from the file is loaded into MHS and is used by ValueOptions staff to verify enrollment in other RBHAs and for ValueOptions providers to verify that a consumer is enrolled with ValueOptions. ValueOptions loads the full State Roster on Monday and the incremental State Roster Tuesday through Friday to build a historical State Roster file. A file is produced daily from the CIS system, RBHA enrollment, and AHCCCS eligibility files that have been created or updated during the nightly batch run.

The State Roster is comprised of several components:

- Incremental Statewide Enrollment Roster,
- RBHA Enrollment Record, and
- AHCCCS Eligibility Record.

The full statewide enrollment roster file, produced weekly from the CIS system, contains all occurrences of RBHA enrollment and AHCCCS eligibility that have been created or updated during the week

Purpose/Uses:

This file/extract is used to verify consumers that are already enrolled in the state BHS system and to see if a consumer is enrolled in ValueOptions or another RBHA. The file is used to verify if a consumer has a CIS number currently assigned to them and to verify the correct spelling of names, social security numbers and date of births.

Name	Data Type	Length	Description
Record Type	char	1	Record Type
Client identification number	char	10	CIS Consumer Number
Change Control Date	char	8	Date Last Changed
AHCCCS Identification Number	char	9	Consumers AHCCCS ID
Social Security Number	char	10	Consumers Social Security Number
Client First Name	char	10	Consumers First Name
Client Last Name	char	15	Consumers Last Name
Client Date of Birth	char	8	Consumers Date of Birth
Client Gender	char	1	Consumers Gender
SMI Flag	char	1	SMI Flag
SED Flag	char	1	SED Flag

Table/Extract: ALTCS File

Description:

ALTCS Extract file - Long Term Care Consumer information is a weekly file from AHCCCS containing consumer information. The file is downloaded and loaded into the ValueOptions data warehouse. The data is run against MHS to verify that ALTCS consumers are correctly identified. Several reports are generated from this data.

Purpose/Uses:

This file is used to verify whether a consumer is on the ALTCS Roster. ValueOptions runs the file against MHS to see if any of the consumers that are currently enrolled in MHS are ALTCS consumers.

Name	Data Type	Length	Description
AHCCCS Identification Number	char	9	Consumers AHCCCS ID
Client's Last Name	char	20	Consumers Last Name
Client's First Name	char	10	Consumers First Name

Name	Data Type	Length	Description
Client's Middle Initial	char	1	Consumers Middle Initial
Client's Date of Birth	char	8	Consumers Date of Birth
Client's Enrollment begin date	char	8	Consumers Enrollment Date
Client's Enrollment end date	char	8	Consumers Expiration Date
Health Plan identification	char	6	Consumers Health Plan
Site	char	2	Site identifier

Table/Extract: REFER01 - Reference File 1

Description:

These are monthly files from AHCCCS, containing AHCCCS procedure code information. These files are used to verify service codes and gender-specific and age-specific requirements. The data from these files are downloaded monthly from the FTP server and loaded into the data warehouse. The data from these files are used to edit ValueOptions claims before they are paid in MHS, and before being sent to CIS.

The file is transmitted with a variety of record types. Each record type is stored in a separate table within the data warehouse. The record types include: Demographic, Max Allowed Charge, AHCCCS Coverage, AHCCCS Medical Category of Services, Revenue Code to Bill and Revenue to Procedure Code.

Purpose/Uses:

This file is used as a resource to validate data (error checking). ValueOptions uses this file to verify that the services provided for our consumers meet all the criteria required by AHCCCS for that service code. Age, gender, and category of service are validated against program parameters.

REFER01 - Reference File 1 record type - Demographic

Name	Data Type	Length	Description
Procedure Code	char	5	Service Code
Description	char	65	Service Code Description
Minimum Age Limitations	char	3	Minimum Age limitations
Minimum Age Type	char	1	Minimum Age Type
Maximum Age Limitations	char	3	Maximum Age Limitations
Maximum Age Type	char	1	Maximum Age Type
Record Type	char	2	Record Type Indicator

REFER01 - Reference File 1 record type - Max Allowed Charge

Name	Data Type	Length	Description
Procedure Code	char	5	Service Code
County	char	2	County Available
Begin Date	char	8	Service Code Begin Date
End Date	char	8	Service Code End Date
MAC	num	13	Specialty Code
CRN Date	char	8	Creation Date
Record Type	char	2	Record Type Indicator

REFER01 - Reference File 1 record type - AHCCCS Coverage

Name	Data Type	Length	Description
Procedure Code	char	5	Service Code
Coverage Code	char	2	Coverage Code
Replacement Procedure Code	char	6	Replacement Service Code
Begin Date	char	8	Service Code Begin Date
End Date	char	8	Service Code End Date
Record Type	char	3	Record Type Indicator

REFER01 - Reference File 1 record type - AHCCCS Medical Category of Service

Name	Data Type	Length	Description
Category of Service	char	2	Category of Service
Category of Type	char	1	Category of Type
Category of Service From	char	11	Category of Service From
Category of Service To	char	11	Category of Service To
Beg Date	char	8	Category of Service Begin Date
End Date	char	8	Category of Service End Date
Record Type	char	2	Record Type Indicator

REFER01 - Reference File 1 record type - Revenue Code to Bill Types

Name	Data Type	Length	Description
Revenue Code from	char	3	Service Code From
Revenue Code to	char	3	Service Code Thru
Bill type from	char	3	Bill Type From
Bill type to	char	3	Bill Type Thru
Error Code	char	4	Error Code
Revenue 3 rd DGT indicator	char	1	Revenue 3rd DGT indicator
Coverage Indicator	char	1	Coverage Indicator
Unit Indicator	char	1	Unit Indicator
PA Code	char	1	PA Code
Medicare Review Indicator	char	1	Medicare Review Indicator
Manual Procedure Indicator	char	1	Manual Procedure Indicator
Procedure Indicator	char	1	Procedure Indicator
Beginning Date of Service	char	8	Beginning Date of Service
Ending Date of Service	char	8	Ending Date of Service

REFER01 - Reference File 1 record type - Revenue Code to Procedure Code

Name	Data Type	Length	Description
Revenue Code from	char	3	Revenue Code from
Revenue Code to	char	3	Revenue Code to
Procedure From	char	3	Procedure From
Procedure to	char	5	Procedure to
Beginning Date of Service	char	8	Beginning Date of Service
Ending Date of Service	char	8	Ending Date of Service

Table/Extract: REFER02-Reference File 2

Description:

These are monthly files from AHCCCS containing AHCCCS procedure code information. These files are used to verify service codes, gender specific and age specific requirements. The data from these files is downloaded monthly from the FTP server and loaded into the data warehouse. The data from these files is used to edit ValueOptions claims before they are paid in MHS,

and before being sent to CIS. The file is transmitted with a variety of record types contained within the file. Each record type is stored in a separate table within the data warehouse. The record types include Procedure and Modifier.

Purpose/Uses:

This file is used to validate claims in the claims adjudication process. This file verifies the maximum units allowed for a certain service. The file is used also used to verify valid service codes.

REFER02 - Reference File 2 record type - Procedure

Name	Data Type	Length	Description
Procedure Code	char	5	Procedure Code
Description	char	14	Description
Start Date	char	8	Start Date
End Date	char	8	End Date
Maximum Units	char	3	Maximum Units
Frequency Value	char	3	Frequency Value
Frequency Code	char	1	Frequency Code
Anesthesia Maximum	char	4	Anesthesia Maximum
Anesthesia Value	num	5	Anesthesia Value
Maximum Allowable Charge	num	13	Maximum Allowable Charge
Follow Up Period	char	3	Follow Up Period
Gender	char	1	Gender
Minimum Age	num	3	Minimum Age
Minimum Age Qualifier	char	1	Minimum Age Qualifier
Maximum Age	num	3	Maximum Age
Maximum Age Qualifier	char	1	Maximum Age Qualifier
Medicare Coverage Indicator	char	1	Medicare Coverage Indicator
Record Type	char	2	Record Type Indicator

REFER02 - Reference File 2 record type – Modifier

Name	Data Type	Length	Description
Procedure Code	char	5	Procedure Code
Procedure Modifier	char	2	Procedure Modifier
Payment Type	char	2	Payment Type
Amount	num	15	Amount
Begin Date of Service	char	8	Begin Date of Service
End Date of Service	char	8	End Date of Service
Claim Receipt	char	8	Claim Receipt
Record Type	char	2	Record Type Indicator

Table/Extract: Provider

Description:

The data from this file is used as a reference to validate provider type combined with category of service. The file is downloaded from the FTP server on a monthly basis and is loaded into the data warehouse. The record types include Demographic Record, Enrollment Status, Category of Service, Payment Rate, License, Specialty, Medicare, Restriction, Address, Address2 and Address3.

Purpose/Uses:

This file is used during a checking process to ensure that a provider is eligible to provide specific services. This file also identifies what types of services a certain provider can provide and during what period of time. This file also identifies the category of services, provider types and demographic information of the provider. This file is provider specific.

Provider record type - Demographic Record

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Provider Name	char	25	AHCCCS Provider Name
Provider Type	char	2	AHCCCS Provider Type
IHS Indicator	char	1	IHS Indicator
Record Type	char	2	Record Type Indicator

Provider record type - Enrollment Status

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Provider Status Type	char	1	AHCCCS Provider Type
Provider Status	char	2	AHCCCS Provider Status
Begin Date	char	8	AHCCCS Effective Date
End Date	char	8	AHCCCS Expiration Date
Replacement Provider ID	char	6	Replacement Provider ID
Record Type	char	2	Record Type Indicator

Provider record type - Category of Service

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Category of Service	char	2	AHCCCS Category of Service
Begin Date	char	8	Effective Date
End Date	char	8	Expiration Date
Record Type	char	2	Record Type Indicator

Provider record type - Payment Rate

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Service Type	char	1	AHCCCS Service Type
Service Form	char	11	AHCCCS Service From Date
Service To	char	11	AHCCCS Service To Date
County	char	2	County
CRN Date	char	8	CRN Date
Begin Date	char	8	Begin Date

End Date	char	8	End Date
Name	Data Type	Length	Description
Rate Schedule	char	3	Rate Schedule
Payment Type Values	char	1	Payment Type Values
Amount	char	11	Amount
Record Type	char	2	Record Type Indicator

Provider record type - License

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Agency	char	3	Agency
License Identification Number	char	15	Provider License Number
License Certification Indicator	char	2	Provider License Certification Indicator
Begin Date	char	8	Begin Date
End Date	char	8	End Date
Record Type	char	2	Record Type Indicator

Provider record type - Specialty

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Specialty	char	3	Specialty
Begin Date	char	8	Begin Date
End Date	char	8	End Date
Record Type	char	2	Record Type Indicator

Provider record type - Medicare

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Medicare Coverage	char	1	Medicare Coverage
Medicare Identification Number	char	10	Medicare Identification Number
Carrier Identification Number	char	5	Carrier Identification Number
Intermediary Code	char	5	Intermediary Code
Begin Date	char	8	Begin Date
End Date	char	8	End Date
Record Type	char	2	Record Type Indicator

Provider record type - Restriction

Name	Data Type	Length	Description
Provider Identification Number	char	5	AHCCCS Provider Number
Service Type	char	1	Service Type
Service From	char	11	Service From
Service To	char	11	Service To
Begin Date	char	8	Begin Date
End Date	char	8	End Date
Restriction Type	char	2	Restriction Type
Agency Identification Number	char	3	Agency Identification Number
Record Type	char	2	Record Type Indicator

Provider record type - Group Affiliation

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Group identification Number	char	6	Group identification Number
Affiliation Begin Date	char	8	Affiliation Begin Date
Affiliation End Date	char	8	Affiliation End Date
Record Type	char	2	Record Type Indicator

Provider record type - Address

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Address Type	char	1	Address Type
Locator Code	char	2	Locator Code
Street Address 1	char	25	Street Address 1
Street Address 2	char	25	Street Address 2
Beg Date	char	8	Beg Date
End Date	char	8	End Date
Record Type	char	2	Record Type Indicator

Provider record type - Address 2

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Address Type 2	char	1	Address Type 2
Location Code 2	char	2	Location Code 2
Pay Location code	char	2	Pay Location code
City	char	25	City

County	char	2	County
Name	Data Type	Length	Description
State	char	2	State
ZIP	char	9	ZIP
Country	char	2	Country
Business Phone	char	10	Business Phone
Emergency Phone	char	10	Emergency Phone
Record Type	char	2	Record Type Indicator

Provider record type - Address 3

Name	Data Type	Length	Description
Provider Identification Number	char	6	AHCCCS Provider Number
Address Type 3	char	1	Address Type 3
Location Code 3	char	2	Location Code 3
Tax identification Number	char	20	Tax identification Number
Attn	char	25	Attn
Record Type	char	2	Record Type Indicator

Table/Extract: Profile

Description:

The file is downloaded from the FTP server on a monthly basis and is loaded into the data warehouse. The data from these files is used to edit ValueOptions claims before they are paid in MHS, and before being sent to CIS.

Purpose/Uses:

This file is used during a checking process to ensure that a provider is eligible to provide services. It also identifies what types of services a certain provider can provide and during what period of time.

Name	Data Type	Length	Description
Provider Type	char	2	AHCCCS Provider Type
Category of Service	char	2	AHCCCS Category of Service
Mandatory/Optional	char	1	Mandatory/Optional
Service From	char	11	Service From
Service To	char	11	Service To
Service Type	char	1	Service Type
Effective Begin Date	char	8	Effective Begin Date
Effective End Date	char	8	Effective End Date
Record Type	char	2	Record Type Indicator

All requirements of the proposal regarding to data mapping and storage are currently fully implemented under our current contract as the RBHA.

k. Data Flows and System Edits

ValueOptions believes in maintaining a high level of data integrity, which we achieve by continually devoting time and resources to enhance our systems and processes. Through developing more efficient data flows and by applying accurate data edits that reduce data entry errors and minimize rework, we are able to improve productivity as well as provide data that is reliable and accurate. We believe that better quality control from the beginning means a more dependable, efficient system and contributes to better business operations overall.

Currently, ValueOptions collects seven major categories of data, including Enrollment, Eligibility, Demographic, Crisis, Registration of Care, Customer Service, and Claims Information. Within these categories exist sub-groups of data such as Housing, SMI Determination, and Grievance and Appeals information. Each is described later in this section and is presented with accompanying flow charts to assist with the visualization of the basic process.

As we grow with Maricopa County, we will continue to look for new ways to streamline the flow of data, making it even more efficient and timely.

Data Flows

ValueOptions collects a significant amount of data from its contracted providers—even more than what is required for any given contract. Our primary purpose for this data collection is to provide measurable data used to improve care, ensure equitable delivery of care across the spectrum, and to identify the types of care needed by a specific population. By constantly measuring the outcomes of our efforts, we are able to see where we can improve, as well as to identify what factors are making a difference.

In our current role as the Maricopa County RBHA, we collect enrollment and disenrollment, demographic, crisis, authorization and claims information as required under this contract. Details of these data flows are outlined in the sections below.

Enrollment, Disenrollment and Demographic Processing

As the following figure, 5k.1, illustrates, intake providers' enrollment and demographic information has traditionally arrived at ValueOptions in one of two ways. Those utilizing third party software submit a file extract which, after being verified, is loaded into our MHS system, while those lacking the technical capability fax completed enrollment and demographic forms to ValueOptions' EAD Department, where they are manually keyed into the system.

Providers submitting electronically are offered an internally developed application at no cost, which allows them to compare their data to various formatting edits, enforced by ValueOptions—this quality control measure is called “scrubbing.” The provider then submits the file electronically in the HIPAA 834 format where it is re-verified by ValueOptions' internal data scrubber.

ValueOptions also created a HIPAA compliant Electronic Data Interface (EDI), which providers can download at no cost. For those who otherwise would have to submit paper claims due to lack of technical resources, this application provides an easy way to create HIPAA compliant electronic files.

In either case, providers receive an error report documenting the details of any record failing these initial edits and are responsible for fixing and resubmitting them. A second scrubber then reformats accepted records for submission to MHS, which, in turn, forwards them to CIS, Arizona's Client Information System. CIS then generates an accepted/erred file indicating which records were accepted and which were denied. MHS flags all accepted records accordingly, while denied records are researched, fixed and resubmitted by the EAD Department. Relevant reporting tables within the data warehouse are updated accordingly, and providers are notified of their data submission performance via reports that are posted to PRIDUS for their download and review.

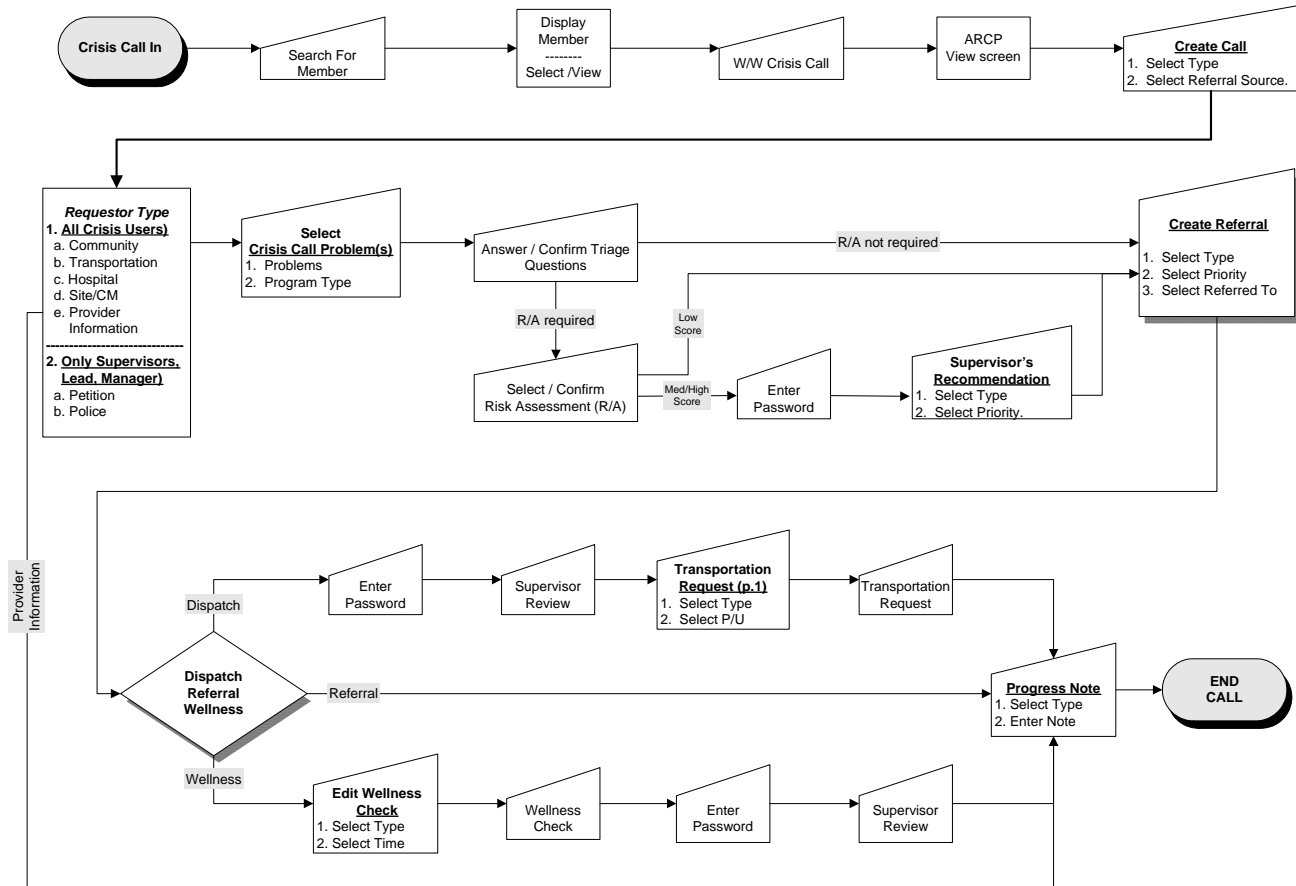
The planned rollout of ValueOptions' web-based enrollment and demographic forms in December 2003 will introduce significant efficiencies to this process, pushing electronically submitted enrollments and assessments from 29% and 30%, respectively, to upwards of 80%. This push to minimize—if not eliminate paper forms, in conjunction with electronic submission over a secure medium, yields increased privacy, while simultaneously reducing downstream administrative and processing costs associated with error handling. Future phases will seek to implement an increasing percentage of edits at the

user interface level, further minimizing downstream processing costs, as well as the ability for end users to submit field specific edits online.

Crisis

ValueOptions currently provides the only countywide crisis call center. This call center collects critical information on eligible and non-eligible consumers for the immediate delivery of crisis services, for fire and/or police dispatch, and for mobile crisis team dispatch. Our Crisis module team not only provides a systemic way to dispatch immediate care to those in need; it also provides our organization with the data necessary to analyze where additional urgent and specialized care centers may be needed. Following (Figure 5k.2) is a condensed flow chart of how the crisis module data flows.

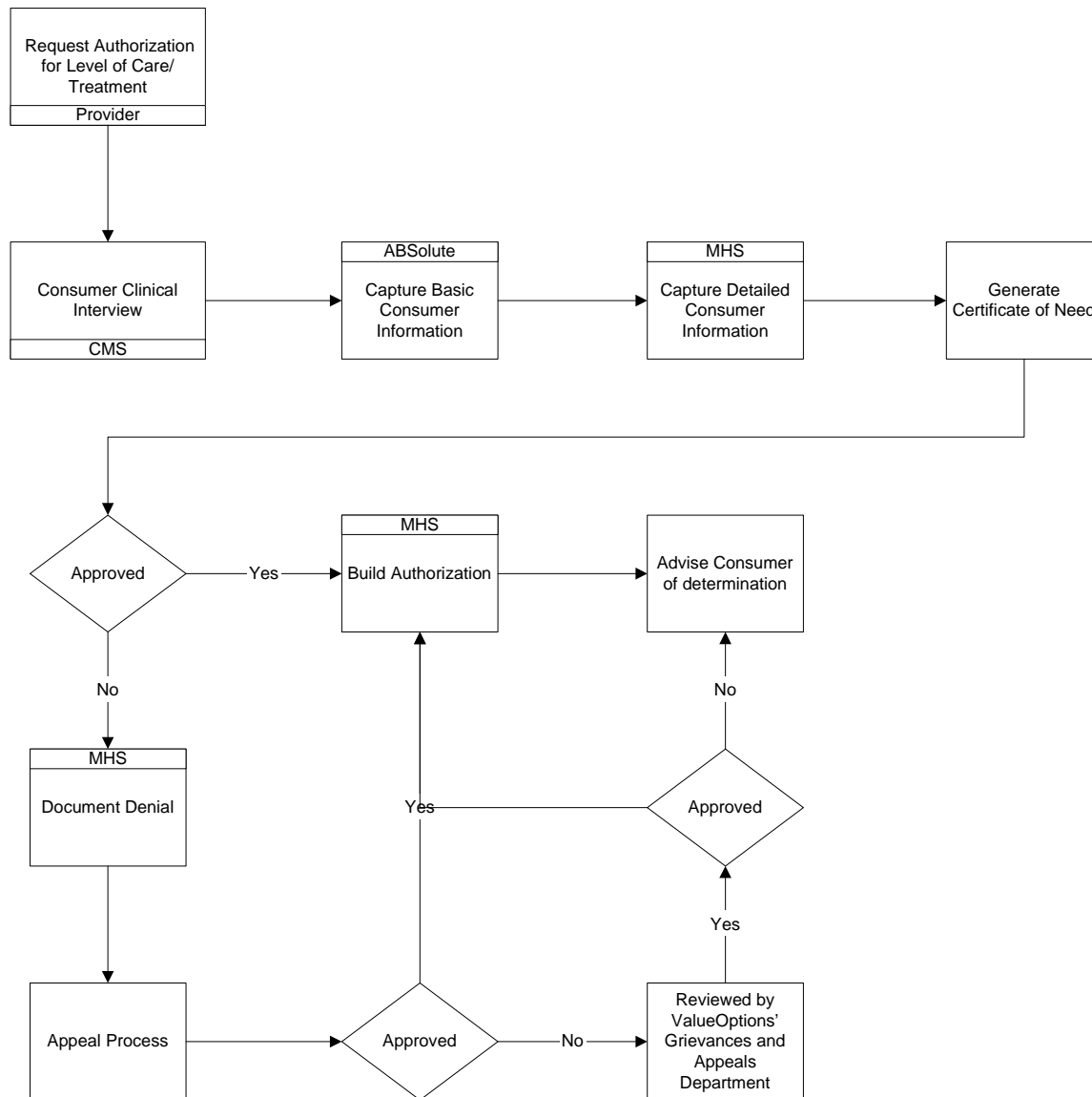
Figure 5k.2 Crisis Data Flow



Registration of Care

ValueOptions currently utilizes the e-provider module and an IVR system, described earlier in *Section 5.b.*, to register some adult outpatient care. This system is user friendly and allows providers to call a toll-free number, register the consumer, and request up to a certain amount of units of care based on the service code. For the higher levels of care (Inpatient, RTC, and others), ValueOptions requires providers to call our Access line and request the higher level of care through a documented registration process (Figure 5k.3). ValueOptions reviews the request and processes as appropriate, based on the clinical needs of the consumer.

Figure 5k.3 Authorizations



Customer Service

ValueOptions provides a well-designed customer service inquiry-tracking module for staff to record and capture customer service calls. These calls range from general questions to specific issues with treatment. All calls are recorded and tracked based on the type of call received. These systems ensure that the critical customer service functions are efficient and informative for our providers and consumers.

Claims Submission and Processing

ValueOptions continues to ensure the prompt and accurate processing of its providers' claims through the utilization of a series of checks and balances designed to expedite their adjudication and payment. Related reporting capabilities then ensure that claims disposition is conveyed to providers as quickly and accurately as possible. The commitment to assisting providers in this process is nowhere more evident than in the deployment and maintenance of the EDI Claims Link application to any interested provider since its rollout in 1999. Less than 3% of all claims are now submitted on paper, and ValueOptions of Arizona boasts the lowest average cost per claim of any ValueOptions' Service Center across the country. In the last year alone, increased automation in the area of claims processing has seen average processing costs drop by 27%. Furthermore, the percentage of claims auto adjudicated has risen significantly, from 50% during the contract's first two years, to 91% last fiscal year. Limited only by the fact that provider checks are cut weekly, the average turnaround time per claim now stands at six days.

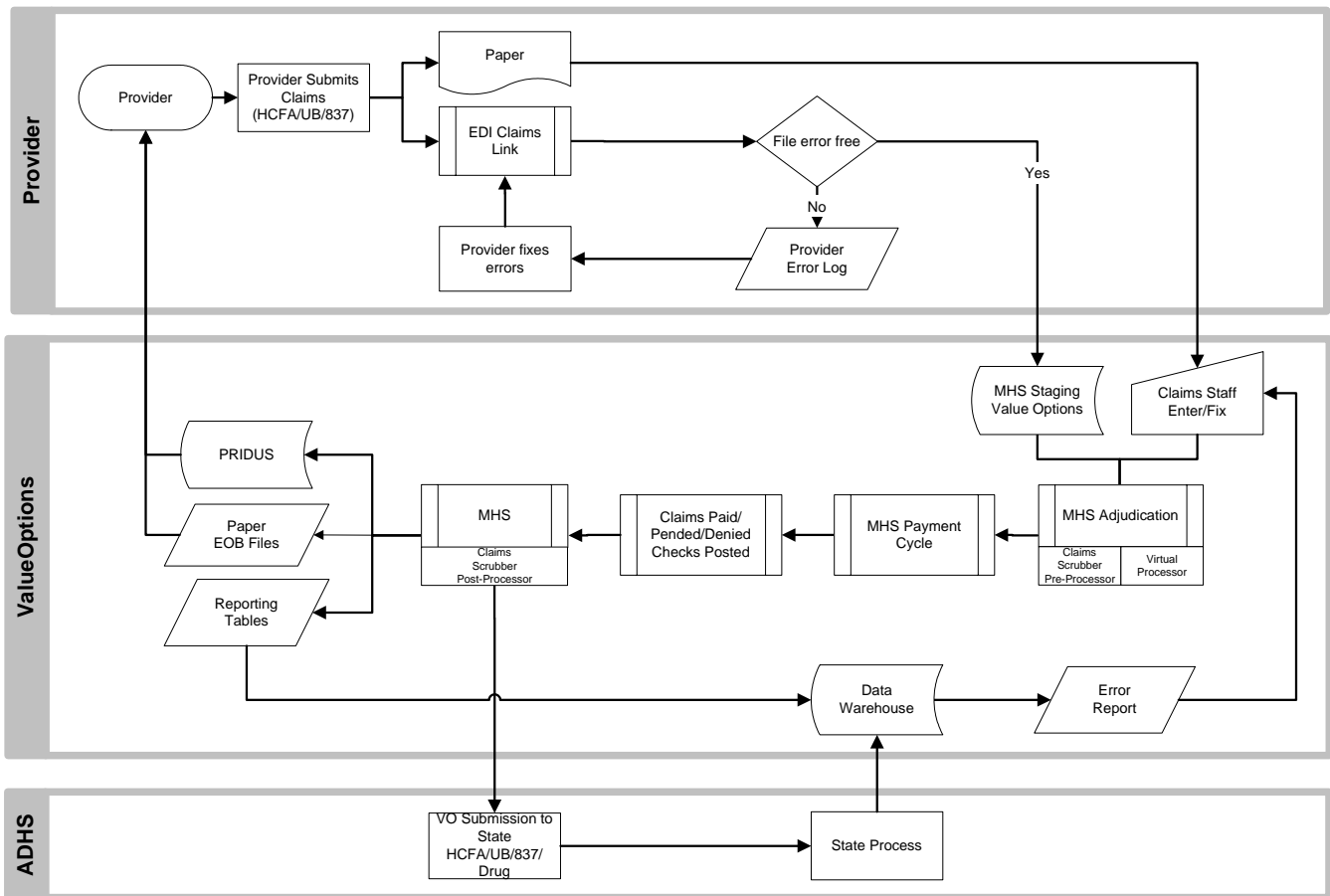
As the following Claims Submission and Processing Data Flow diagram (Figure 5k.4) illustrates, providers submit claims to ValueOptions via one of two mediums, paper or electronic. It is the electronic scrubber that performs the first in a series of ValueOptions' data edits and validation, verifying that 97% of claims passing through it satisfy established rules with regard to field length, values and record count. Provider files generating 25% in related errors are returned to the submitting provider(s) for correction. "Passing" files are forwarded to the MHS staging area.

At this point, the electronic claims enter a second series of edits in which those failing to meet MHS formatting requirements are marked for denial. All electronic claims are then uploaded to MHS. Meanwhile, Claims Processing staff key the limited number of paper claims submitted directly into MHS.

All claims are then adjudicated and assigned a "Denied", "Pended" or "Adjudicated" status based upon standard business edits. This process is followed by the more stringent application of a subset of Arizona-specific claims edits—a process mentioned earlier called "scrubbing"—in which one or more errors result in a claim being marked for denial. Additional automated processing power is then applied in the form of a "virtual processor", an internally developed tool that allows the ad hoc application of a predefined set of actions to a specific claims set, enabling the automatic dispensation of thousands of claims—otherwise handled manually—in a fraction of the time. The synergy of the three processes, adjudication, scrubbing and virtual processing is illustrated when, for example, claims assigned "A" status ("adjudicated") in the adjudication process, but failing to pass local edits, are automatically processed as denials, pends, etc. The virtual processor, by itself, offers an added advantage, in that it allows ValueOptions to automatically reverse claims submitted by providers in error, for example, those where a service is billed improperly.

When the adjudication is complete, Claims Processing staff updates MHS accordingly, and then release "paid" claims for payment. At this point, all claims undergo yet another scrubbing, wherein those submitted by ValueOptions' sub-contractors are marked for internal processing, while those to be forwarded to our contractor, DBHS, undergo further comparison to edits specific to that contract. EOB files are then sent to ValueOptions' providers in two formats, paper and electronic. The first is mailed, while the second is posted to PRIDUS, ValueOptions' web-based information server, for easy access by providers. Claims specific to ValueOptions' state contract are then forwarded to CIS for processing, yielding an accepted/rejected file report, which is then pulled into our data warehouse. Claims staff then work any rejected files accordingly. Records of all transactions are maintained in ValueOptions' data warehouse reporting tables.

Figure 5k.4 ValueOptions Arizona Claims Submission and Processing



CIS-Client Information System
 PRIDUS - Provider Reporting Information Download/Upload Server
 MHS - Managed Healthcare System
 EDI - Electronic Data Interchange

Edits Applied

ValueOptions' comprehensive network of management information systems has an extensive and complex editing capability; however, it is flexible enough to allow for unique contract and client management edits that are applied under the current contract as the Maricopa County RBHA. Based on current requirements of the contract and this proposal, there are more than two hundred specific edits within the HIPAA compliant file transmission process alone. These edits have enabled ValueOptions to move claims submission rates from 14% of claims submitted within 45 days in 1999, to over 75% today. In addition, auto-adjudication improved from less than 50% to more than 93% today.

Moving forward, ValueOptions continues to facilitate provider submission rates and data accuracy through bi-monthly training, software enhancements, complimentary technical support and process improvement teams. In addition, ValueOptions has sponsored a claims summit where "hands-on" claims and billing staff meet with senior Claims Processing and Information Systems staffs to discuss issues, challenges, and ideas for system enhancements. The following flow charts summarize the editing process and the main edits within our VMIS system.

Figure 5k.5 Edits

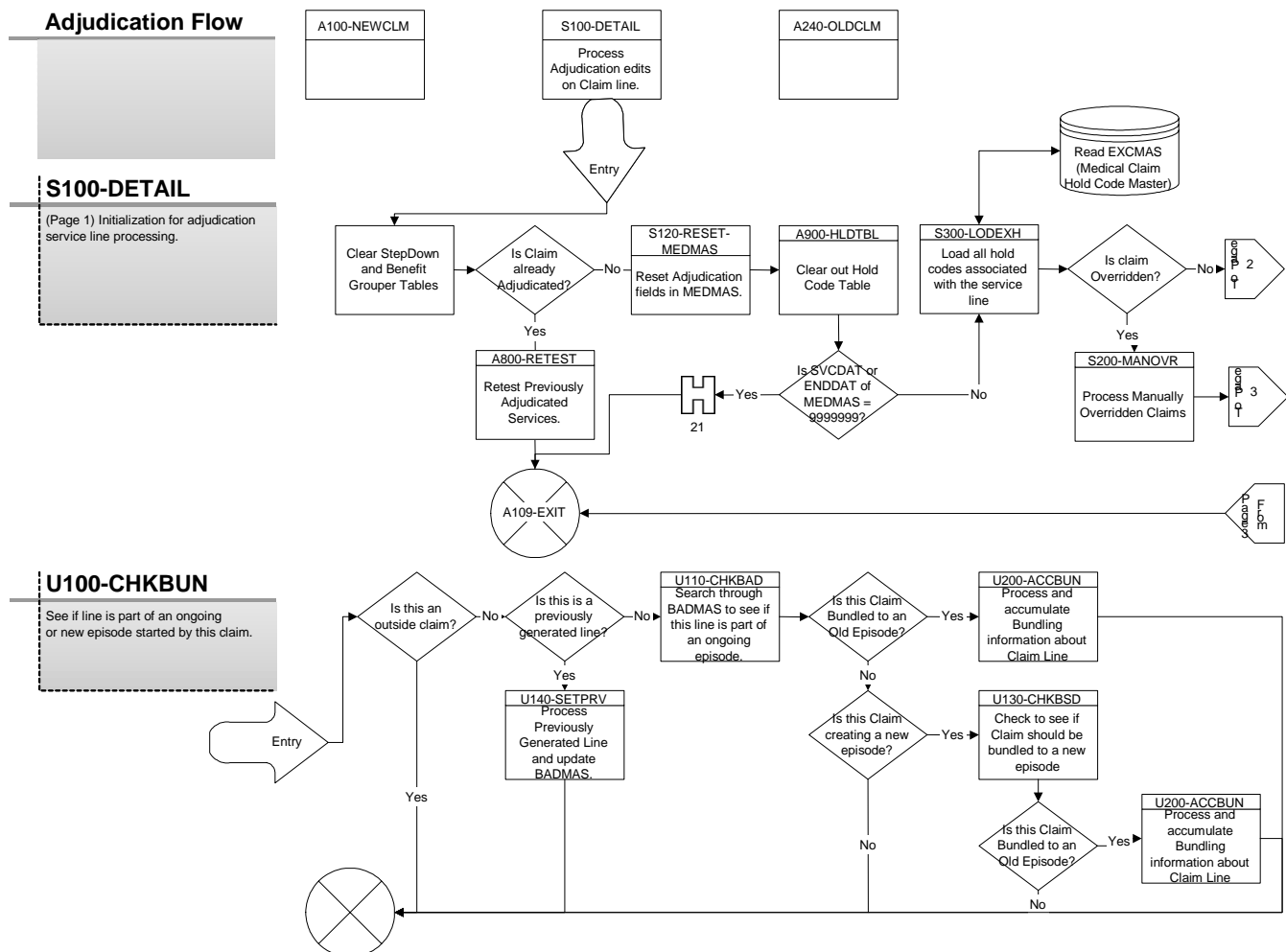
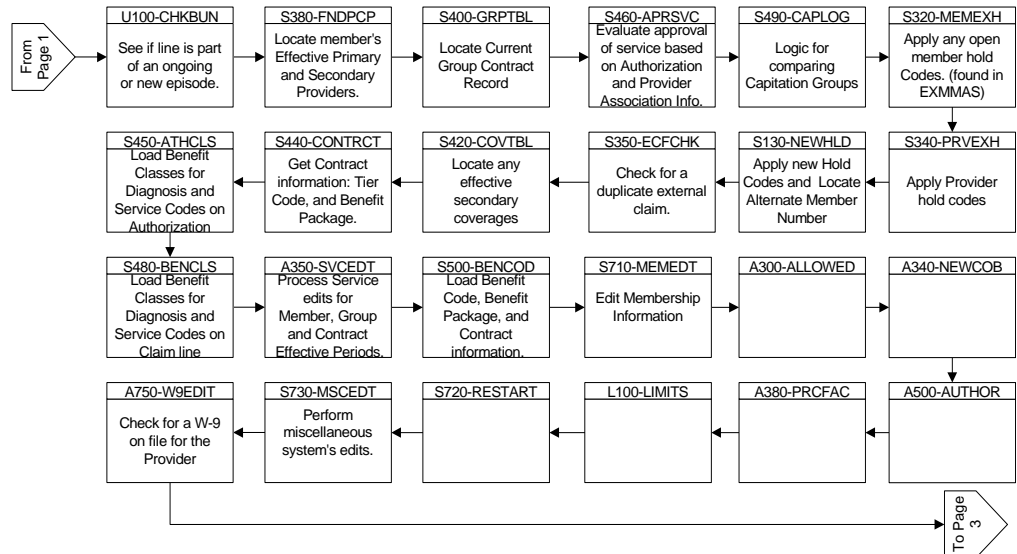


Figure 5k.5 Edits (Continued)

S100-DETAIL

(Page 2) Process adjudication edits on claim service lines logging any hold codes that may be produced.



U100-CHKBUN

See if line is part of an ongoing or new episode started by this claim.

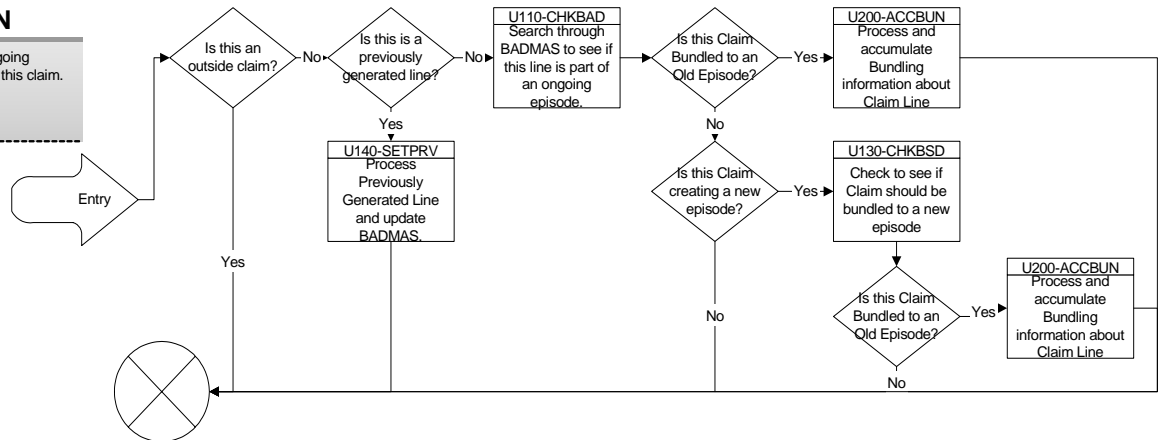


Figure 5k.5 Edits (Continued)

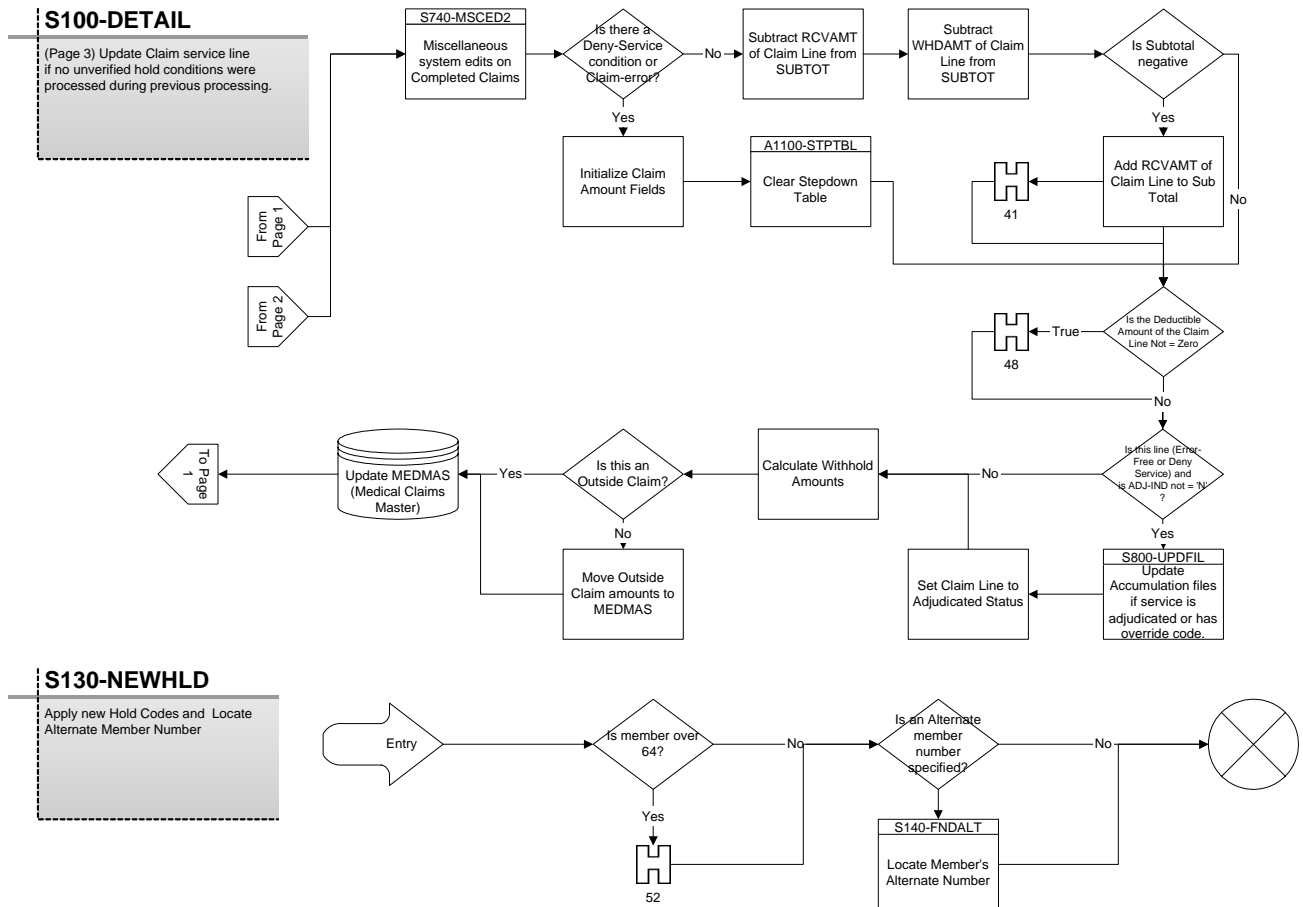


Figure 5k.5 Edits (Continued)

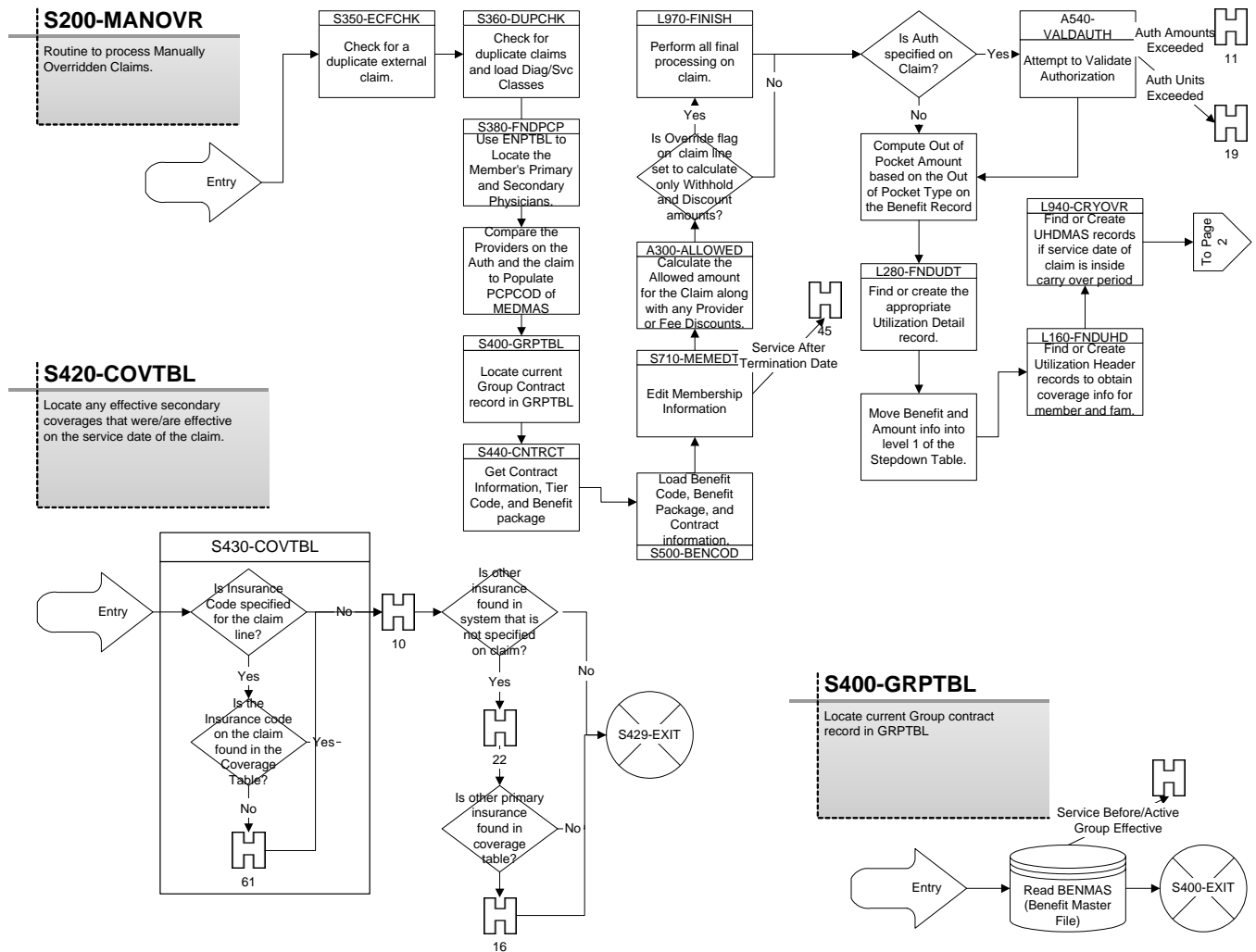


Figure 5k.5 Edits (Continued)

S200-MANOV

(Page 2) Process Unit, Deductible, Copay, Coinsurance, Coverage, Out of pocket and Episode groupers.

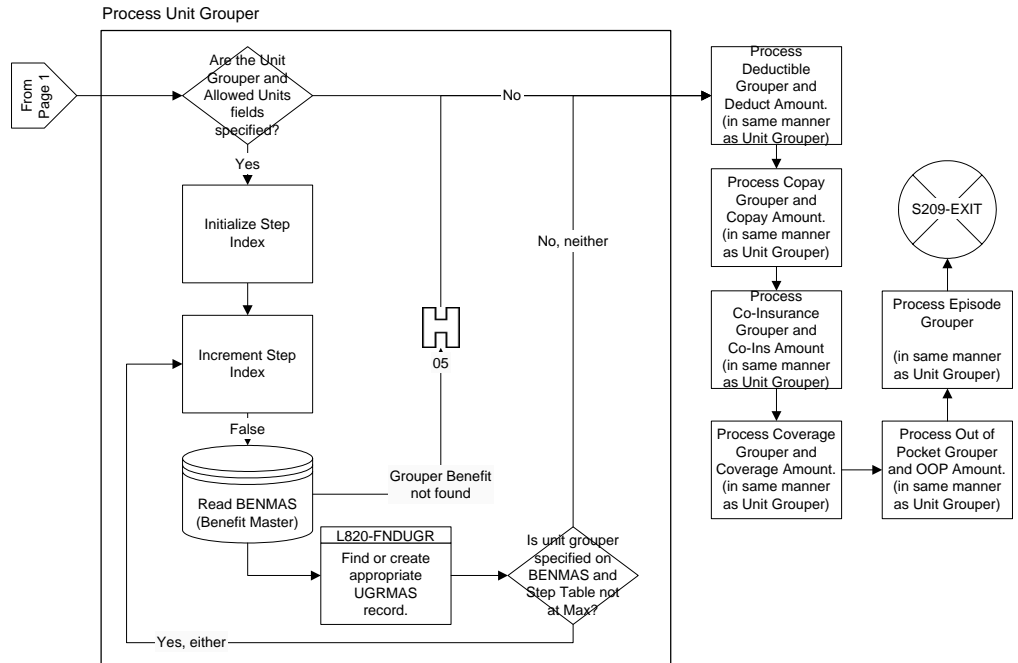


Figure 5k.5 Edits (Continued)

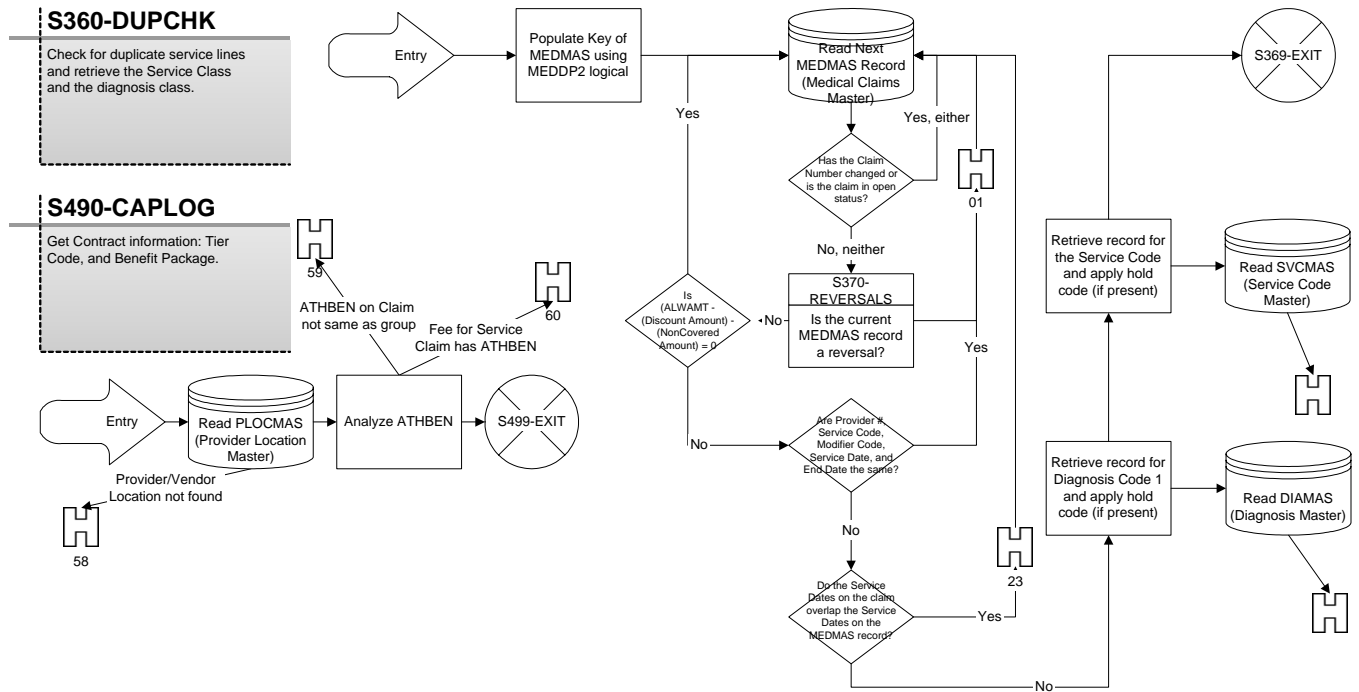


Figure 5k.5 Edits (Continued)

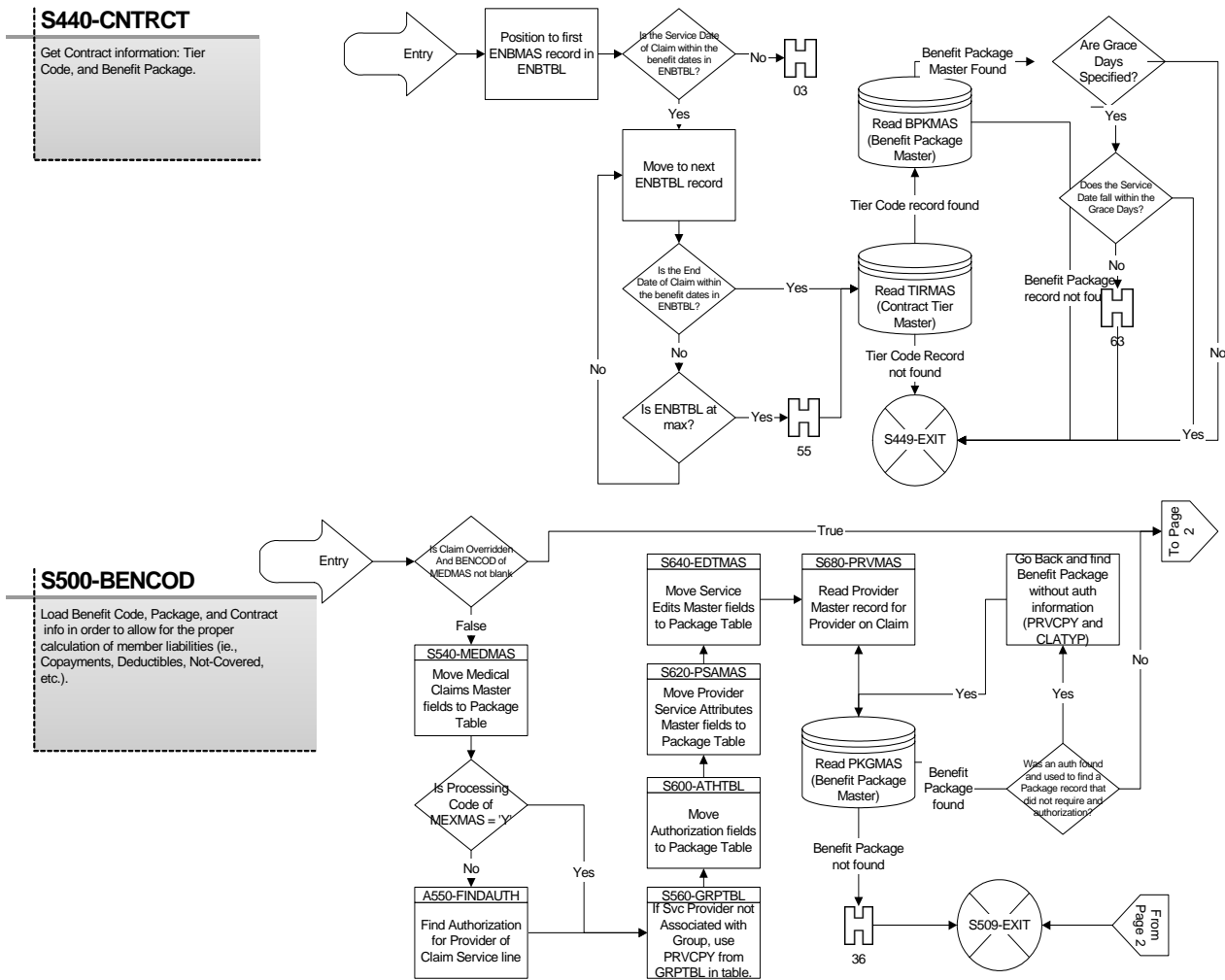


Figure 5k.5 Edits (Continued)

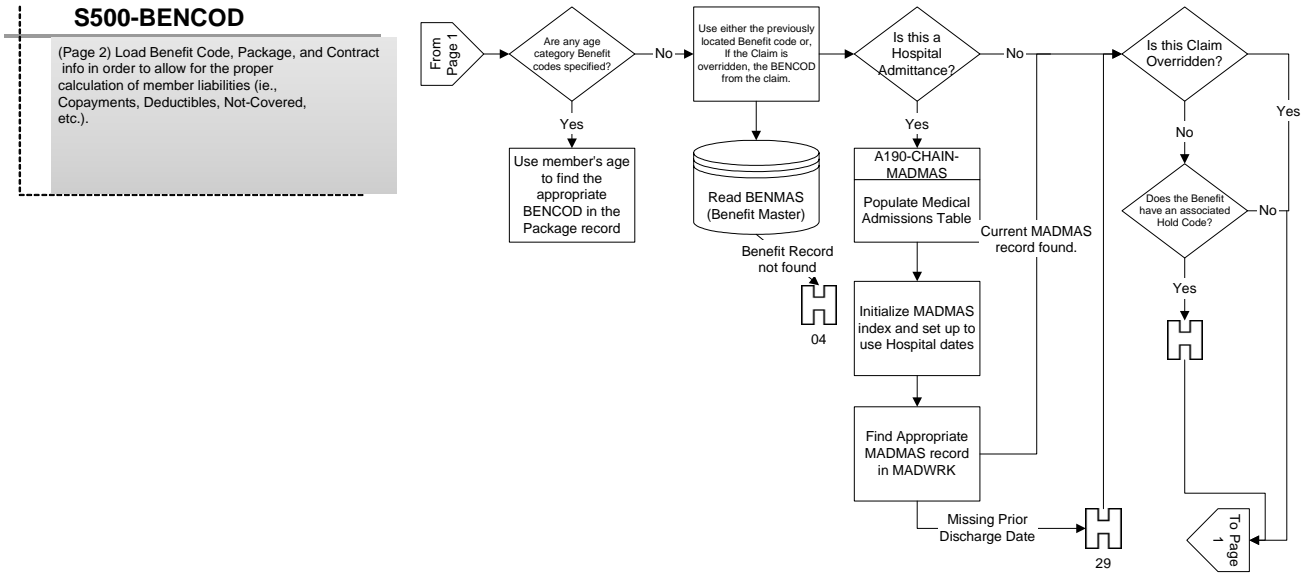
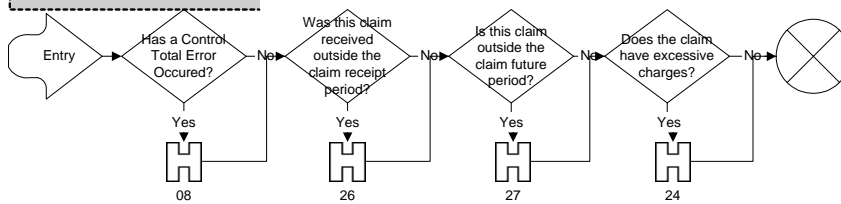


Figure 5k.5 Edits (Continued)

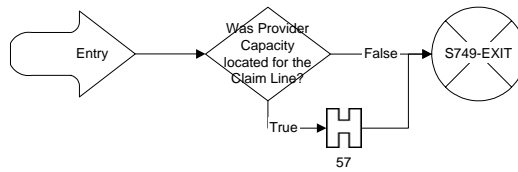
S730-MSCEDT

Perform miscellaneous system's edits.



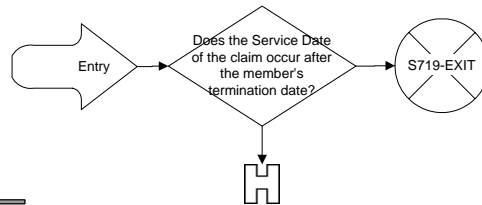
S740-MSCED2

Miscellaneous system edits on Completed Claims: Check to see if provider capacity is specified.



S710-MEMEDT

Edit Membership Information.



S750-W9EDIT

Check for a W-9 on file for the Provider. This edit is only performed when the Provider is being paid.

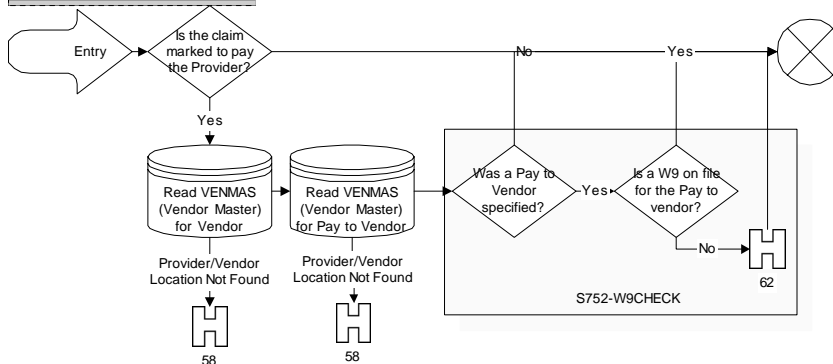
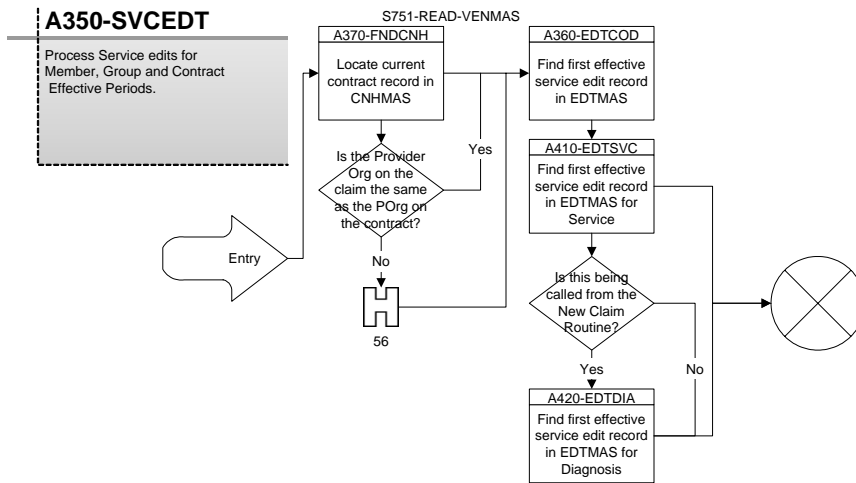


Figure 5k.5 Edits (Continued)



I. Testing Plan and Data Conversion

As the Regional Behavioral Health Authority (RBHA) for Maricopa County, ValueOptions has successfully passed all testing and data conversion requirements contained within this Request for Proposal (RFP), the CIS File Layout Specifications Manual, the ADHS Program Support Policy and Procedure Manual, and the Office of Grievance and Appeals Database Manual. We are also the first RBHA to achieve compliance with all HIPAA requirements with regards to our electronic data interchange with the ADHS/DBHS. We are continuously developing more thorough ways of testing and monitoring our processes for ways to improve.

ValueOptions stands ready to present a system readiness review, upon award of the Maricopa County contract, to demonstrate how our extensive ValueOptions Management Information Systems (VMIS) can meet and exceed the State requirements and needs stated in this RFP.

Testing Plan

Upon award of the contract, ValueOptions will immediately compile all requirements, any modifications to those requirements made by the ADHS/DBHS, and any additional standard posted after the RFP submission date to include with the following testing scenario.

Item	Description	Start Date	End Date	Comments
1	Re-verify All Data Requirements, to include a finalized mapping of required data elements being collected, stored, and transmitted.	2 Feb 04	8 Feb 04	<ul style="list-style-type: none"> CIS File Layout Specifications Manual ADHS Program Support Policy and Procedure Manual All other items identified within RFP Any additional requirements
2	Re-verify “live” transmissions of all HIPAA transactions to ADHS/BHS.	2 Feb 04	9 Feb 04	<ul style="list-style-type: none"> 834 Enrollment 837P Professional 837I Institutional NCPDP Drug Format Gain Letter of Status Pass/Fail from ADHS/BHS
3	Re-verify “live” transmissions of all additional electronic transactions to ADHS/BHS	9 Feb 04	11 Feb 04	<ul style="list-style-type: none"> Demographic Data File Gain Letter of Status Pass/Fail from ADHS/BHS
4	Make required modifications to Data Requirements as needed	12 Feb 04	25 Feb 04	<ul style="list-style-type: none"> Resend to ADHS/BHS in test format Gain Letter of Status Pass/Fail from ADHS/BHS
5	Make modifications to main systems/web apps/site for data collection if needed.	12 Feb 04	25 Feb 04	<ul style="list-style-type: none"> Test with providers under Level I, Level II, and Level III testing.
6	Update Business Continuity Plans, policies, and procedures as needed.	12 Feb 04	26 Feb 04	<ul style="list-style-type: none"> Document Final Processes
7	Seek ADHS/BHS Pass/Fail of Readiness Review.	27 Feb 04	27 Feb 04	<ul style="list-style-type: none"> Request Letter of Compliance relating system meets requirements.

Our process for demonstrating compliance with the testing requirements in each area is defined in the next few pages. This covers our main system development on the AS400, MHS Cyclical Release Procedures, Development Implementation Checklist – MHS Production File Conversions, and Testing Strategy. We then describe our Data Warehouse Application Development, Reporting and Testing Process, and finally present our Level 1, Level 2, and Level 3 testing flow and requirements.

AS400 Development Process

Our development group has created standardized procedures for project and design request creation, movement of program modifications to production, program-naming standards, modification of MHS source code, physical and logical file creation as it pertains to Implementer, program archiving, and test environment cleanup. ValueOptions uses the industry's leading change management software application, "Implementer," to ensure, through a series of tracking and change management features, that promotion and deployment processes cannot be compromised. The following is a breakdown of our main areas relating to the AS400 development process:

Project and Design Request Creation

A project and design request is created in Implementer for each new task. A manager and programmer's initials are required for each project that is identified, along with a brief description of the project and a description of each task within the project. Each project is separate and self-contained, to create manageable and easily tested and reversed segments. When the promotion is complete, all programs within a design request are then moved together. A status code is assigned to a design request automatically as it is created and promoted through Implementer. A Manager then approves the request and changes the status to "A1" prior to sending the request to production. The Manager's update of the status code serves as the final approval for the move. A request cannot be staged until the status has been modified. Lastly, only a manager can create an emergency project.

Move of Program Modifications to Production

When using Implementer to promote programs to a production or test environment, we use a target environment group if a program or file needs to reside in more than one library. Once a program has been promoted to another environment, no additional changes can be made to that program. To modify the program, the reject function must be used to move the program back to the test library. If the program is not sent back to the test library prior to making changes, Implementer will not allow the project to continue on to production. When the programs have been staged, Implementer generates a request report, and this report must be printed out and attached to the ValueOptions Systems and Programming Production Change form. Both a hard copy and a soft copy of the ValueOptions Systems and Programming Production Change form is required for all moves.

This form is then moved to a designated folder on our mainframe, where it is saved in accordance with standard naming conventions. All move paperwork must be to the Source Control Manager by 12:00PM and have complete sign off as shown in the ValueOptions Systems and Programming Production Change form. If the information required for a move to production is not complete, the programs will not be moved into production. The Application Owner must approve any move request that needs to be put into production on a weeknight that is not eligibility related. All move requests will be put into production by the Source Control Manager, System Operator or Programmer on call.

Creating/Changing Files

A File Change Request form must be completed prior to modifying a database file, and then sent to the AS/400 Database Administrator. Any file changes made to the MHS system requires notification to be sent out to several other departments by the Database Administrator. New physical and logical files may be checked and promoted through Implementer. Some file changes can be performed through Implementer, but this is only done on a case-by-case basis and with approval of the Source Control Manager.

Archiving and Development System Clean up

During the testing process, to ensure business continuity and to protect the source code, no archive copies of the source code are kept in any of the production libraries. Instead, the source code is stored in archival libraries and managed through our change management controls. Any programs not checked through Implementer that remain in the test environments on the development system are removed. An automated clean-up process is run after a release. This process moves any illegal programs to one of the designated holding libraries until the process is run again. Each time the process is run, the holding libraries are cleared and all of the programs and objects in those libraries are removed. Programmers check these libraries prior to each release for any programs that might have been removed that they want to save.

MHS Cyclical Release Procedures

The development group has also created a standardized procedure for cyclical MHS releases, and for keeping all other Information Services Departments and Service Centers informed of release information and testing in a timely manner. These notifications are in a standardized and easy-to-understand release documentation format, including detailed descriptions of the programming changes and screen prints to give end users a visual illustration of such changes.

All project tasks for Business Support and Migration will be scheduled on a cyclical release cycle with the following exceptions, which are categorized as “urgent” and uploaded as soon as possible:

- eligibility uploads or extracts,
- priority 1 system down errors preventing users from performing their daily functions,
- bug fixes limited in scope to one service center, priority 2 in nature affecting end users ability to perform job functions, or having the potential to corrupt data, and
- client specific uploads and extracts with contractual obligations before the next cyclical release.

The following guidelines will be adhered to for purposes of cyclical releases:

- file conversions will only be performed quarterly (potentially 3/31, 6/30, 9/30, 12/31),
- only 1 adjudication change per release with the exception of bug fixes,
- only 1 finance change per release with the exception of bug fixes,
- test scripts must be developed and distributed for all testing levels inclusive of programmer Level 1 testing, and
- changes to requirements identified during testing are documented in functional specifications and the revision log entry is filled out according to change management

The following activities and timeframes detail how release information is categorized and distributed:

Step	Activity	Time Frame	Responsible Party
1	80% list of release information sent to Business Support and MHS+ in spreadsheet format	30 days prior to code drop	Technical Project Manager
2	Distribution of 100% release list to Business Support and MHS+ and freeze of functional coding changes	2 weeks prior to code drop	Technical Project Manager
3	Place all programs and files for release in the standard production environment	30 days prior to code drop	Source Control Manager, Development team
4	Level 2 signoff must be obtained and distribution of changes to service centers for Level 3 testing (except bugs)	30 days prior to code drop	Business Analyst
5	Notification of file changes to IVR, Data Warehouse, Reporting	4 weeks prior to code drop	Database Programmer Analyst
6	Final list of enhancements verified to Testing and Documentation	Monday COB prior to weekend code drop	Business Analyst
7	Pull any enhancements that will not go and notify Business Support.	Noon Tuesday prior to weekend code drop	Development Manager

Figure 5L.1 Snapshot of Sample MHS Release Procedures

MHS Cyclical Release Procedures							
FUNCTION							
	One Service Center or Client		Multiple Service Centers/Clients				
DOC. DELIVERY PERIOD	Online & Select Screens, Menus	Batch Programs	Online & Select Screens, Menus	Batch Programs	Eligibility Conversion and Upload program	Bug Fixes. No end user change-batch or online	Adjudication. Enhancement changes
Release Notes. Monday prior to Move	Y	Y	Y	Y	N	Y	Y
Business Impact Document. 2 Weeks prior to move. 1 week lead time to prepare	N	N	Y	Y	N	N	Y
Level 2 signoff. 30 days prior to move	N	N	Y	Y	N	N	Y
Executive approval. Non-weekend moves	Y	Y	Y	Y	N	Y	N/A
Global Service Center. Signoff	N	N	Y	Y	N	N	Y
Testing Unit Involvement	N	N	Y	Y	N	N	Y

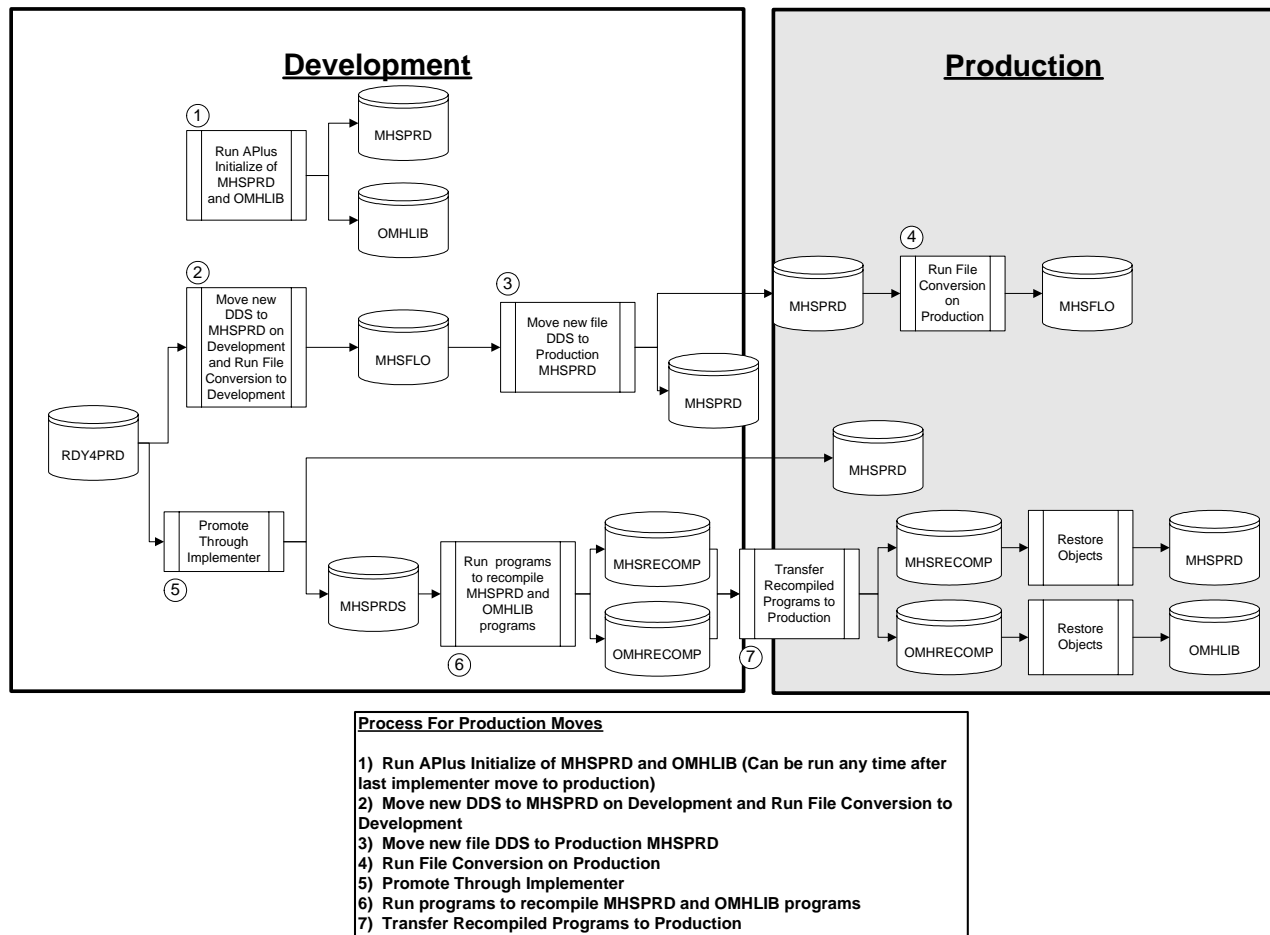
Development Implementation Checklist – MHS Production File Conversions

To ensure that each step of the testing process is completed and to provide a high level of quality control, ValueOptions Information Services Department uses a detailed, extensive checklist. A copy of this checklist is provided below.

Function	Resource	Target Date	Status
Initial Setup			
Identify final list of projects for implementation			
1-Week prior to implementing into production, notify VOICE via e-mail of the pending changes and down time			
1-Week prior to implementing into production, Notify Senior Management and Claims Management of impending down time			
Announce source code freeze in RDY4PRD			
Create on-call list for Saturday programmers and consultants			
Prepare Production Move Signoff forms for all projects to be moved			
Obtain signatures and emails for business signoff			
Ensure Release Notes have been sent to Helpdesk			
RDY4PRD Staging			
Stage all Implementer requests and give staged move requests to operations			
Implementation Day			
Recompile queries on Production			
Check all submitted jobs to make sure that the programs modified on the release have not affected the job run parameters. (AO4071)			
Perform programmer and analyst testing on Production machine			
Perform user testing on production machine			
Receive user signoff			
Notify Operations and ABS departments that signoff has been received and the users can get back on the system			
Clean Up – Development and Production AS/400s			
Delete data files in RDY4FL* that are now in production			
Clean up RDY4PRD, RDY4TST, and RDY4WKLY libraries			
Check for program source and objects			
Ensure that all documentation is up to date and in the correct location			
Clean up Re-compile libraries. MHSRECOMP, OMHRECOMP, RDY4RECOMP			
Delete all file conversion work files and backup files on Development and Production systems			

Preparation for Next Release			
Promote RDY4TST projects to RDY4PRD for the next release.			
Back Out Plan			
Page IT Directors			
Notify Critical Contacts			
Restore Backup files			
Back out all program changes			
Retest			
Lets users on system and open IVR			

Figure 5I.2 Functional View of MHS Development and Production Integration



Testing Strategy

This section covers Level 2 integration testing, Level 3 testing, the fix-retest cycle, signoff on test results and the transition strategy for corporate development projects.

Level 2 Integration Testing

Integration testing ensures that modified programs continue to interface correctly with partner programs and with internal and external systems. This testing is performed on all changes/enhancements to ValueOptions' systems to confirm that the change satisfies the requirements of the original request and to ensure that performance and response times are within acceptable parameters. Typically, quality assurance testers from the Systems Training, Testing and Documentation department perform integration testing. If the subject matter of the enhancement or scope of the project is outside the testers' expertise, subject matter experts from elsewhere in the company can be requested to perform the testing.

Integrated testing consists of up to four phases, not all of which are applicable in every case:

1. **Request Overview** – a brief summary of the business requirements that led to the change request.
2. **Function Test** – a detailed description of the procedures necessary to verify that each function yields the desired result and performs within specifications.
3. **Performance Test** – a detailed description of how to run speed trials to ensure that the resulting programs are fast enough to meet the requestor's needs.
4. **Enterprise Assimilation Testing** – a detailed description of how to test the programs at the system level for any negative repercussions.

The Test Lead determines the combination of phases that are applicable to a change/enhancement based on the complexity and scope of the change.

Ten Typical steps in Integration Testing follow:

1. The Test Lead acquires a copy of the Level 2 test plan, as well as a copy of the functional and technical specifications applicable to the change/request.
2. The Test Team, most often the quality assurance testers, reviews the test plan and defines a structured approach to the testing.
3. The Test Lead makes a task list and assigns team members to each task on the list. The task list also establishes the testing milestones within the timeframes for Level 2 testing defined in the test plan. If necessary, the Test Lead contacts staff members from other departments to participate in the testing.
4. The Test Lead confirms that the team has access to the test environment, programs and data called for in the test plan.
5. The testers responsible for performing the tests run the functional, performance and enterprise assimilation scenarios described in the test plan.
6. The Test Lead schedules a daily meeting with the testers to monitor the progress and address any issues.
7. If all programs perform as expected, the tester documents their findings on the test plan and completes the Test Sign-off form.
8. If the testing reveals unexpected or unknown problems, the tester documents their findings using the bug list (an application, called OnTrack, set up to automatically notify the programmer of an error via email). The tester provides the Test Lead with any necessary hardcopy supporting documents. The Programmer then makes the necessary correction(s).
9. The Test Lead oversees the fix-retest cycle, as necessary, until the problem is resolved and the tester accepts the change/enhancement.
10. If the testing reveals a problem that results in changes to the specifications, the test plan changes accordingly and affects subsequent Level 1 and 2 testing.

Once all Level 2 testing is complete, the Test Lead and Test Manager sign the Test Sign-off form. The following table is an example of Level 2 test specifications:

Level 2 Test Specifications

Test Plan Details and Purpose:			Hardware/Software Requirements:		Bug Report Process:	Retest Process: (See fix-retest cycle diagram)
	Test Scenario	Expected Results	Actual Results	Test Data (Claim #, Auth #, Consumer #, etc.)	Comments/Issues	Pass/Fail
1.	Type in Action to check for Action code setup in RU1161. Verify all valid Action Codes are listed. Verify action codes match with what's listed in the functional spec.	All Action codes for screen are listed and match action codes defined in spec.				

Procedures for Data Management and Analysis (DMA) testing include the following five steps:

1. A Programmer creates a report based on the specifications prepared by an analyst on a Technical Specification Request (TSR) form. When the Programmer finishes creating the report, he or she executes the report to verify that it runs to completion in a reasonable amount of time. The programmer also checks to see that the calculations are correct and that all the required fields appear on the report. This testing is analogous to Level 1 testing described elsewhere in this document.
2. The Programmer gives the report and TSR back to the initial analyst who documented the business requirements and wrote the specifications. This analyst runs a series of in-depth tests designed to verify how the report selects and groups data (by age bracket or service code, for example), and calculates totals. This testing, analogous to Level 2, requires at least three scenarios using various sets of parameters meaningful to the report. The analyst checks the accuracy of the report in each case and documents their findings on the TSR Validation Checklist.
3. Level 2 testing continues as the first analyst passes the report to another analyst, one that was not involved in the project initially. This second analyst begins the testing process by reviewing the report documentation and the TSR to understand the nature of the report. They then select and run one of the test scenarios to verify that both iterations produced the same results. Finally, the second analyst designs and runs new scenarios to test other aspects of the report, they then update the validation checklist accordingly.
4. Once the second analyst verifies the report's accuracy, he or she passes the report to the DMA Quality Control Analyst, who checks to see that the report's number (ID), pagination, fonts, and general presentation are correct. The Quality Control Analyst then updates the validation checklist. This phase is the last of Level 2 testing (Level 2B testing). The following table is an example of Level 2B testing:

Level 2 B Test Specification

Project Title		Testers	System	Files/Screens Involved	Test Dates	Abbreviations Legend
	Test Scenario	Expected Results	Actual Results	Test Data (Claim #, Auth #, Consumer #, etc.)	Comments/ Issues	Pass/Fail
2.	Check format of screen title	Title of screen centered, white, all uppercase. All fields in line 2 enclosed in 'box'.				

5. Once this internal testing is complete, DMA delivers the report to the requesting department or service center with instructions to run the report and verify its accuracy. This is analogous to Level 3 testing.

Level 2 testing always involves use of the test plan developed by the Test Team. The test plan details the purpose of the testing, participants, testing scenarios (including entrance and exit criteria), expected results, the hardware/software requirements, the bug reporting process, and re-test procedures.

Level 3 Testing

Level 3 testing does not begin until Level 1 and 2 testing are complete. If there are unresolved discrepancies from Levels 1 and 2, the Test Lead and Lead Programmer can decide that it is appropriate to proceed with Level 3 testing if the unresolved discrepancies are deemed inconsequential. Unaddressed prerequisites and conditions previously identified by the Test Team can also prevent Level 3 testing from proceeding.

Level 3 testing, or User Acceptance Testing (UAT), can range from relatively simple to very complex. The scope and magnitude of the enhancement or project determines the nature of the subsequent UAT. For example, if the change is the creation of a new report, user acceptance requires little more than having the user run the report and verify that it contains the requested information. If the enhancement is a major project involving multiple programs and functions, UAT consists of a tightly orchestrated Model Office (parallel) simulation, where users test all business processes using production data, as they would in performing their daily tasks. The Test Lead determines the exact format of Level 3 testing.

Level 3 testing always involves use of the test plan developed by the Test Team. The test plan details the purpose of the testing, participants, testing scenarios (including entrance and exit criteria), expected results, the hardware/software requirements, the bug reporting process and re-test procedures. The test plan also identifies a point of contact for all testers, typically the Test Lead.

Basic User Acceptance Testing, performed when the enhancement is relatively simple in nature, contains the following seven steps:

1. The Test Lead acquires a copy of the Level 3 test plan.
2. The Test Lead sends the plan to the user(s) designated to participate in the process.
3. The Test Lead contacts the user(s) to review the plan, provide training, answer any questions and schedule the start date. This point of contact can be in person, via email or by phone.
4. The user(s) responsible for performing the tests run the scenarios described in the test plan.
5. If all programs perform as expected, the tester documents his/her findings on the test plan and completes the Test Sign-off form.
6. If the testing reveals unexpected or unknown problems, the tester documents his/her findings using the OnTrack software. The tester provides the Test Lead with any necessary hardcopy supporting documents. The Programmer then makes the necessary correction(s).
7. The Test Lead oversees the fix-retest cycle, as necessary, until the problem is resolved and the tester accepts the change/enhancement.

When the scope of the enhancement is complex, this process typically calls for Model Office or parallel testing. In Model Office testing, the goal is to simulate, to the degree possible, an actual working business environment using the modified system and a copy of the production data. Model Office testing employs users who will be using the modified system in their day-to-day operations. Throughout the Model Office exercise, the Test Team monitors the users' activities and facilitates the test process.

The following list details the ten steps necessary to prepare for and implement Model Office testing:

1. The Test Lead confirms the test location, equipment availability, and test environment/data and staff member availability for the planned dates of the testing. The Test Lead also provides the requesting department representative with copies of the approved test plan.
2. The Test Lead confirms the training needs of the users/testers. The testers must be familiar with the scope of the project and understand how the project impacts their daily workflow. If on-site training is necessary, the Test Lead arranges for the training prior to the start of Model Office.
3. The testers must also be familiar with the issue logging process and understand the importance of thoroughly documenting all discrepancies.
4. The Test Lead schedules daily meetings with the applicable Information Services employees during Model Office to review and prioritize bugs found during the testing.
5. The Test Lead schedules a Model Office kick-off meeting with all participants in person or by a conference call. The purpose of the meeting is to make sure everyone understands the goal of the testing and the specific role they are to play.
6. The users perform most of the testing during Model Office, running the scenarios in the test plan and comparing the actual results against the expected results. In addition, the test plan instructs the users to run scenarios they normally encounter during the business day that may not be on the test plan. The Test Plan form has a space for testers to describe the scenarios they create.
7. The Test Team is available to assist with miscellaneous problems, answer questions, and generally facilitate the testing process.
8. If all programs perform as expected, the tester documents his/her findings on the test plan and completes the Test Sign-off form.
9. If the testing reveals unexpected or unknown problems, the tester documents his/her findings using OnTrack software. The tester provides the Test Lead with any necessary hardcopy supporting documents. The Programmer makes the necessary correction(s).
10. The Test Lead oversees the fix-retest cycle, as necessary, until the problem is resolved and the tester accepts the change/enhancement.

Fix-Retest Cycle

The Fix-Retest Cycle controls and monitors the resolution process. When an error is encountered during testing, the following four steps take place:

1. The Test Lead and programmer review the problem and the Programmer makes the necessary corrections.
2. Once the programmer finishes the coding, they perform Level 1 testing according to the Level 1 test plan. If the fix fails the testing, the programmer continues to fix/test the problem. If the fix passes the testing, the programmer moves the fixed program to the appropriate environment and updates the test plan. The following table is an example of Level 1 test specifications:

Level 1 Test Specification

Testing Task	Programmer Initials	Date Completed
The program code meets the requirements of the functional specification		
The program code meets the requirements of the technical specification		
The program runs to completion without failure		
Test data exists or has been created, and used to run the program code		

3. The Test Lead initiates Level 2 testing for the fix. If the Level 2 testing uncovers problems, the tester adds a comment to the OnTrack software to alert the programmer of the problem. Responsibility returns to the programmer for fixing the problem. If the fix passes the Level 2 testing, the Test Lead documents that fact with a comment in the test plan and alerts the user/tester that Level 3 testing can resume.
4. The user reviews the bug's history and continues his/her testing accordingly. If the user finds a problem, they document the problem by adding a comment to OnTrack, and the fix-retest cycle begins again. If the fix passes Level 3 testing, the user documents the findings on the test plan and continues with other Level 3 scenarios.

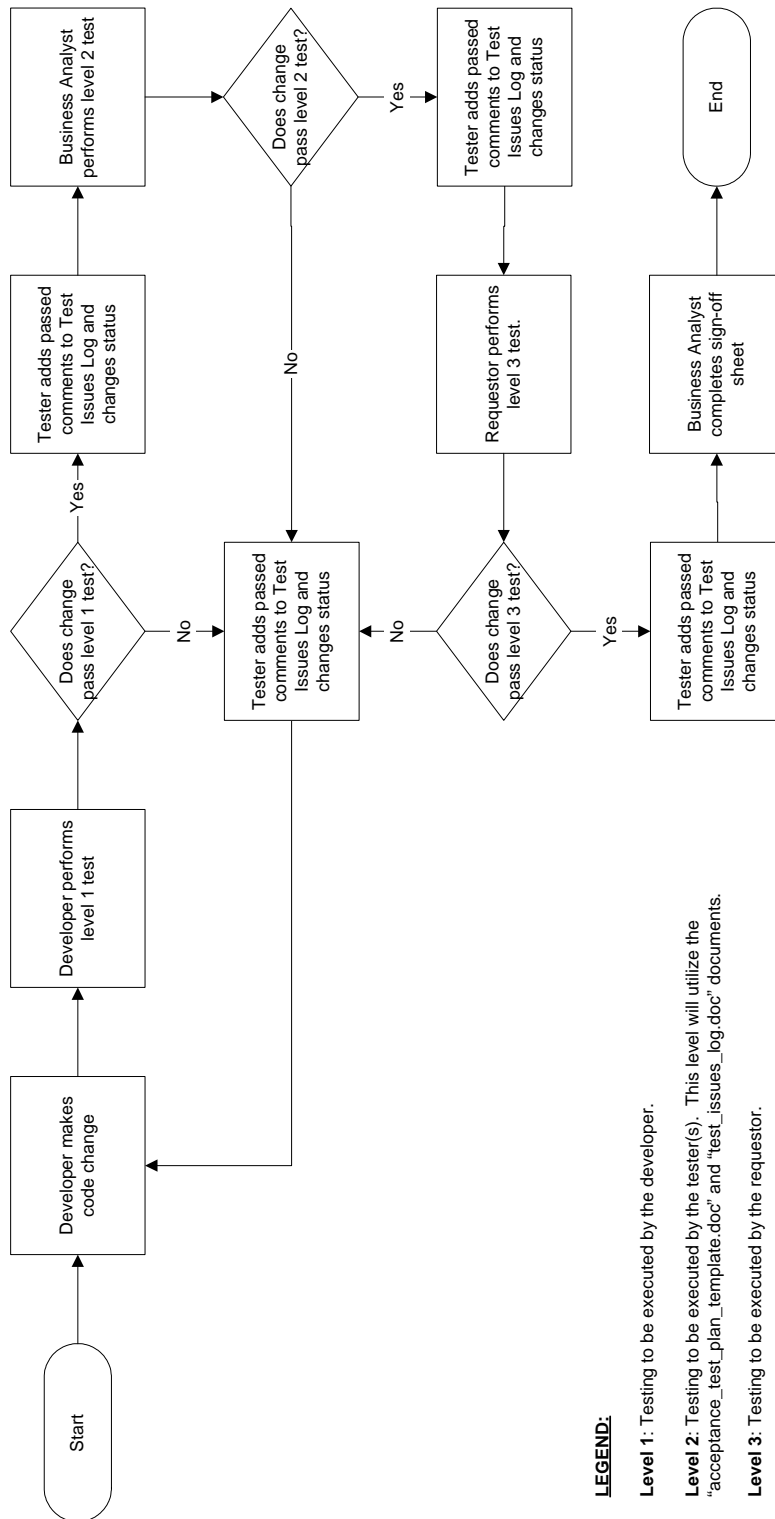
The fix-retest cycle repeats until all problems are resolved or until the Test Lead and customer agree that the problem is not critical to the implementation of the project. The Test Lead prepares a summary document of open issues and attaches it to the project documentation.

Sign-Off and Transition

At the conclusion of testing (Levels 1, 2 and 3), all those involved sign the Initiative Cover Sheet to signify that they approve of the change/enhancement and agree that it should become part of the product.

Once the sign-off procedure is complete and the production readiness planning begins (Change Management), data requirements for implementing the system changes are determined. In preparation for this rollout, the System Training, Testing and Documentation department creates the necessary release notes and submits them to the Chief Technology Officer (CTO) at least 48 hours prior to general distribution. (Note: This step is not required for bug fixes and changes to batch processes.) After the CTO approves the release notes and related system changes, the System Training, Testing and Documentation department arranges for the Technology Call Center to send the release notes to all users.

Figure 5L.3 Fix / Re-test Cycle Diagram



ValueOptions Application Development, Reporting and Testing Process

MIS Development Methodology

The ValueOptions development methodology has four phases: Initiation, Elaboration, Construction and Transition, modeled after the Unified Modeling Language (UML) – an IT industry standard for developing software.

Initiation

The Initiation phase includes the request process, performing an assessment of work requested, alternative options analysis and gathering detailed business requirements.

Requests for application development and report creation are submitted through the Information Services helpdesk. These requests are assigned a unique identification number (the helpdesk ticket number) for tracking. The request can be submitted one of two ways: by calling the helpdesk directly to open a development or report request ticket, or by completing a paper request form, that is then forwarded to the helpdesk for entry into the helpdesk software.

Once a development request has been entered into the helpdesk software, the development team is immediately notified, via email, of the request. At this point, Information Services management reviews the request and assigns a Business Analyst.

The Business Analyst assigned to the project assesses the scope of the project. This entails meeting with the project requester(s) to gather any missing information from the original request, such as system dependencies or boundaries, scalability considerations, specific project objectives and HIPAA considerations. A Work Assessment and Project Scope document is used to record this information and represents the agreement between the individuals responsible for making the request and the Information Services team completing the assessment. The Work Assessment document also addresses high-level resource requirements, the current situation or process, and possible project solutions.

The requestor and Information Services management are required to sign the document to ensure that it accurately reflects the requested effort and to ensure collaboration throughout the Initiation phase of the project.

Alternative analysis is performed by the assigned Programmer and/or Business Analyst, and consists of determining the appropriate solution to meet the requirements. Project scope is revisited at this point. The Alternative analysis includes the following considerations:

- Workarounds or alternatives that can solve the business need more efficiently than the request.
- Available third party products that can solve part or all of the business need, in a more cost effective manner.

Alternatives are documented, and reasons are given for choosing (or not choosing) a solution.

The final step in the Initiation phase is gathering the detailed business and system requirements for the application and/or report. Requirement determination is the result of the Business Analyst working with the customer to determine the business need. The resulting document will be employed throughout the development process, most significantly at the Transition phase, to verify compliance with the requirements. Once the first draft of the document is complete, the Programmer and test coordinator will review this information for clarity, understanding and completeness. The requirements document often undergoes several revisions before it is considered complete. Once complete, the requester must sign off on the requirements before the next phase of development can begin.

The Project Requirements document contains the following information:

- A general statement of project purpose and scope, obtained from the Work Assessment and Project Scope document.
- The intended product use, which includes:
 - Where will the software/report be used?
 - Who are the target users?
 - What is the target hardware/software environment?
 - How long will the solution be used (software that is only produced for short-term needs would be different than something needed for long term use)?
 - How often will the system/report be used (daily, monthly, etc)?
 - Is this application and/or report for an internal audience, external audience, or both?
 - How many total and concurrent users will there be?

- When will the software/report be needed?
- Systems/data sources identified as resources for the request.
- A detailed description of applicable processes/policies/procedures.
- Known interactions with other systems, people, or entities (are there any specific formatting requirements for other systems, people, or entities, i.e. HIPAA)?
- A flowchart or diagram detailing the processes -- not a flowchart of the software design, but a flowchart of any business processes involved, also known as a workflow.
- A detailed explanation of all input and output needed, including needed input fields, categorization requirements and a list of all input, output, and formatting requirements for reporting.
- Project constraints or rules regarding the input (valid ranges of data, lookups required, etc.) and output (size, number of records/pages), fixed deadlines (such as HIPAA compliance dates), and building the project around an existing application, etc.
- Project assumptions (all assumptions on which decisions are based).
- A definition of Security Controls/Audit Trail requirements including requirements for network access, firewall considerations, system access and permissions, system response to changes etc.
- Identifiable resource considerations, such as people, hardware or software needs for the project.
- Error processing requirements (how the program is to handle errors).
- Project approach decisions (buy versus build, use of system versions, etc.).
- Project support processes before, during and after deployment.
- Risk assessment, which includes a list of any “show-stoppers” and the mitigation plan for each.
- Outstanding issues, such as unanswered questions or concerns of the project -- included making the development staff aware of any pending or unanswered issues.
- Project amendments (list the project amendment and the cost to include the new requirement).

The Business Requirements document also requires the signatures of the requestor and Information Services Manager, as the Business Requirements document is essentially a contract between the customer and the Information Services department.

Once the document has been signed, the Elaboration phase of the project can begin. Often, during the course of a project, requirements change. If this happens, the project team must revisit the Business Requirements document to make the necessary adjustments, and gather the required signatures. If the changes are significant, some phases of the project may have to be modified or redone to fit the new requirements.

Elaboration

The Elaboration phase focuses on the initial, detailed software and/or report design, including Entity Relationship Diagrams; prototyping; data specifications; data mapping; security diagrams; and a transition strategy.

Performing software and report design work is essential to the success of the project. Working through the design of the system, or report, prior to construction helps greatly reduce errors in logic, resource utilization, and final design. The design of the system, or report, is the most tangible asset of the project, outside of the actual project deliverable, in that it provides a visual representation of the request and gives the customer, and the development team, the ability to identify problem areas prior to construction.

Entity Relationship Diagrams help the Programmer understand the data, and provide a means to solidify data rules and relationships. Creating an Entity Relationship Diagram also helps identify any additional data elements that need to be captured to comply with the business rules. This process can be done by a skilled Systems Analyst or a Programmer, and is reviewed by a Database Architect.

Prototyping is a required process and must be reviewed and approved by the customer before construction on the project begins. If the request is for application development, the prototype must illustrate the functionality of all user screens and processes within the proposed system. This includes how the system will handle all inputs and outputs. If the request is for reporting the prototype must display the layout, calculations, and data sources for the report. This procedure is the best way to verify our understanding of the project, and ensure the finished product will meet the customer's needs and expectations.

Ensuring the proper security of data and user permissions is a high priority for all applications and reports. Security diagrams are used to test and plan security strategies. System access and security policies and procedures are followed during the design and implementation of security requirements. A transition strategy is developed to identify all impacted groups and coordinate efforts as needed. The transition strategy often includes coordination with training, network operations, help desk and test groups.

A project plan is also developed at this stage, using Microsoft Project 2000 to manage tasks, milestones, resources, and deadlines. The project plan is created by the development team and reviewed by the customer. If the project completion date is not accepted by the customer, and is not negotiable, some items may need to be removed from the project plan to meet the desired deadline.

Construction

The Construction phase encompasses application and/or report programming and sub-testing. Programmers are encouraged to participate in peer reviews during this phase to add an additional layer to the quality assurance of the system. In addition to peer reviews, programmers are required to test application modules and functions as they are developed. Application and/or report construction is based on the approved business requirements and system design.

Test specifications are also developed at this stage. The Business Analyst assigned to the project must complete a test plan document, tailored to the requirements and deliverables of the project. The Test Specification document is used in Level 2 testing, performed by the Business Analyst in a test environment. Any testing issues or failures are recorded in a testing issues document. The complete testing process is described in the next section.

Transition

Finally, the Transition phase is reserved for acceptance testing, training, package and deployment, and post implementation team discussions.

Application and Report testing is performed in three stages: first by the programmer, then by the Business or System Analyst involved in the initiation phase of the project, and finally by the customer prior to deployment. The programmer(s) will test the application and/or report based on the detailed business requirements. The Business or System Analyst testing is based on the Test Specification document (derived from the detailed business requirements). The customer tests the system in the same way that it will be used, which can uncover previously undetected and untested scenarios. If any stage of testing is unsuccessful, the cycle will be repeated.

Testing is complete when all required application and/or reporting functionality has been tested and has produced expected results. If the application and/or report satisfies the original requirements and design specifications (signed off by the customer), the application and/or report is considered complete, and sign off is required from the customer. Any major requirement changes or enhancement requests made during testing will be documented and categorized as either a new project request, or a later version of the program. Minor changes or enhancements (changes that don't interfere with the integrity of the database or the functionality of the program, such as cosmetic changes to forms or reports) can be satisfied without submitting a new request. The following items are verified and approved by the project team prior to report and/or application construction:

- all report groupings and calculations,
- all report data sources,
- all table relationships/links, and
- application and/or report logic.

Deployment includes the release of the software or report, training, and support. This release is completed with the help of the Operations staff, Programming, the Business Analyst, and Training staff. An application and/or report will not be released until all levels of testing have been successfully completed. Direct support on the application and/or report will continue for two weeks after deployment. After that period, correspondence will be routed through the help desk.

Once the project has been successfully deployed and turned over to the help desk, the original project team engages in a "post mortem" session to identify all successful and unsuccessful aspects of the project. This information is then utilized to make improvements to the process.